(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－16565
（P2002－16565A）
(43)公開日　平成14年１月18日(2002.1.18)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ 1/00	Ｆ	５Ｃ０２６
Ｈ０４Ｌ	9/08		Ｈ０４Ｎ 5/63	Ｚ	５Ｃ０６４
Ｈ０４Ｎ	5/63		7/173	６２０Ｚ	５Ｊ１０４
	7/167		Ｈ０４Ｌ 9/00	６０１Ｂ	
	7/173	６２０		６０１Ｅ	

審査請求　未請求　請求項の数17　ＯＬ　（全 33 頁）　最終頁に続く

(21)出願番号　特願2000－199630(P2000－199630)

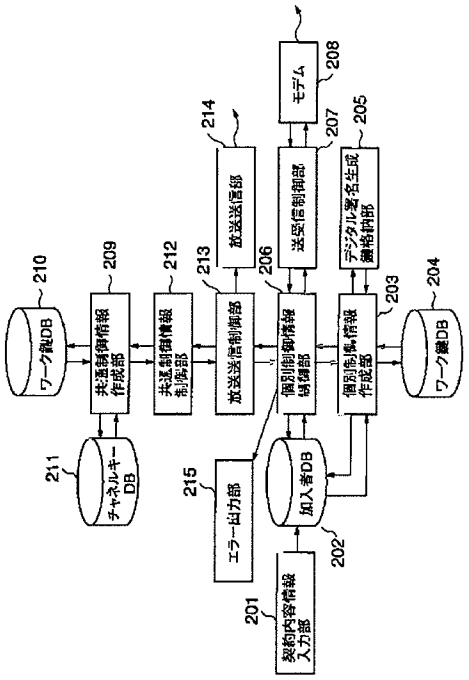
(22)出願日　平成12年６月30日(2000.6.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　情報配信方法および情報配信装置および放送受信装置

(57)【要約】
【課題】加入者が増加しても放送帯域を圧迫することなく、不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。
【解決手段】放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報を復号する受信装置であって前記コンテンツ情報の復号を行うために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記鍵情報を放送配信し、前記受信装置に記憶されている前記復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置との双方向通信により配信し、その際、該受信装置での前記個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信する。



【特許請求の範囲】

【請求項１】　放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の選択および復号を行う受信装置であって前記コンテンツ情報の選択のために必要な前記受信装置に固有の情報を含む制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の選択および復号を行う受信装置に対し、前記鍵情報を放送配信し、前記受信装置に記憶されている前記制御情報の一部または全部を更新するための個別制御情報を前記受信装置との双方向通信により配信し、その際、該受信装置での前記個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信することを特徴とする情報配信方法。

【請求項２】　放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって前記コンテンツ情報の復号を行うために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記鍵情報を放送配信し、前記受信装置に記憶されている前記復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置との双方向通信により配信し、その際、該受信装置での前記個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信することを特徴とする情報配信方法。

【請求項３】　前記受信装置を着信待ち状態にするためのコマンドを放送配信してから前記受信装置を発呼して前記個別制御情報を前記双方向通信により配信することを特徴とする請求項１または２記載の情報配信方法。

【請求項４】　前記個別制御情報を前記双方向通信により配信するために前記受信装置からの発呼を指示するコマンドを放送配信することを特徴とする請求項１または２記載の情報配信方法。

【請求項５】　前記鍵情報を前記受信装置に放送配信される鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化して放送配信することを特徴とする請求項１または２記載の情報配信方法。

【請求項６】　前記受信装置を認証してから前記個別制御情報を双方向通信により配信することを特徴とする請求項１または２記載の情報配信方法。

【請求項７】　放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の選択および復号を行う受信装置であって前記コンテンツ情報の選択のために必要な前記受信装置に固有の情報を含む制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の選択および復号を行う受信装置に対し、前記受信装置に記憶されている前記制御情報の一部または全部を更新するための個別制御情報と前記鍵情報を配信する情報配信装置であって、

前記鍵情報を放送配信する第１の配信手段と、

前記受信装置との双方向通信により前記個別制御情報を配信する第２の配信手段と、

前記個別制御情報の配信先の受信装置で該個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信する第３の配信手段と、

を具備したことを特徴とする情報配信装置。

【請求項８】　放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって前記コンテンツ情報の復号のために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記受信装置に記憶されている前記復号制御情報の一部または全部を更新するための個別制御情報と前記鍵情報を配信する情報配信装置であって、

前記鍵情報を放送配信する第１の配信手段と、

前記受信装置との双方向通信により前記個別制御情報を配信する第２の配信手段と、

前記個別制御情報の配信先の受信装置で該個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信する第３の配信手段と、

を具備したことを特徴とする情報配信装置。

【請求項９】　前記第２の配信手段は、前記受信装置を着信待ち状態にするためのコマンドを放送配信してから前記受信装置に発呼して前記個別制御情報を前記双方向通信により配信することを特徴とする請求項７または８記載の情報配信装置。

【請求項１０】　前記第２の配信手段は、前記個別制御情報を前記双方向通信により配信するために前記受信装置から自装置への発呼を指示するコマンドを放送配信し、その後、前記受信装置からの発呼に応じて前記個別制御情報を前記双方向通信により配信すること特徴とする請求項７または８記載の情報配信装置。

【請求項１１】　前記第１の配信手段は、前記鍵情報を前記受信装置に放送配信される鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化して放送配信することを特徴とする請求項７または８記載の情報配信装置。

【請求項１２】　前記第２の配信手段は、前記受信装置を認証してから前記個別制御情報を配信することを特徴とする請求項７または８記載の情報配信装置。

【請求項１３】　放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う放送受信装置において、

前記放送配信されたコンテンツ情報の復号のために必要な自装置に固有の情報を含む復号制御情報を記憶する記

憶手段と、
この記憶手段に記憶された復号制御情報の一部または全部を更新するための個別制御情報を配信する第１の配信装置から双方向通信によって配信され、あるいは前記第１の配信装置から放送配信された自装置宛の個別制御情報を受信する第１の受信手段と、
この第１の受信手段で双方向通信により自装置宛の個別制御情報を受信したとき、その受領を前記第１の配信装置に送信する受領送信手段と、
この第１の受信手段で受信された個別制御情報に基づき前記記憶手段に記憶された復号制御情報を更新する更新手段と、
前記コンテンツ情報を復号するために必要な全ての前記放送受信装置に共通の鍵情報を配信する第２の配信装置から放送配信された前記鍵情報を受信する第２の受信手段と、
前記記憶手段に記憶された復号制御情報と前記第２の受信手段で受信された鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行うことを特徴とする放送受信装置。
【請求項１４】　放送配信されたコマンドを受信して、前記第１の配信装置から配信される前記個別制御情報を受信可能なように自装置を着信待ち状態にすることを特徴とする請求項１３記載の放送受信装置。
【請求項１５】　放送配信されたコマンドを受信して、前記個別制御情報を受信するために前記第１の配信装置を発呼することを特徴とする請求項１３記載の放送受信装置。
【請求項１６】　前記鍵情報は、別途受信した鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化されていることを特徴とする請求項１３記載の放送受信装置。
【請求項１７】　自装置が前記第１の配信装置から認証された後、前記個別制御情報を受信することを特徴とする請求項１３記載の放送受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、有料放送システムに関する。
【０００２】
【従来の技術】デジタル放送は、通信衛星（ＣＳ）に始まって、ケーブルＴＶ、地上放送へとデジタル化が進むにつれ、一層のサービスの充実が期待されており、これからに放送サービスの主役をつとめていくものと思われる。
【０００３】デジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャネル数の大幅な増加が可能になってことである。更に、高度な誤り訂正技術が適用できるため、高品質で均質なサービスの提供が可能となる。
【０００４】また、デジタル化により従来のように画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして流すことや、ＰＣソフトを放送で配信することが可能となり、そのようなサービスを提供するためのシステムも続々登場してきている。また、受信装置も従来のような据え置き型だけでなく、移動中でも利用できる携帯情報端末、自動車の中での利用を前提とし、自動車に据え付けられている移動端末などモバイル型受信装置も出現している。
【０００５.】このようなシステムにおいて有料放送サービスを実現する際には、放送コンテンツを暗号化して送信し、契約内容に基づいてスクランブルを解くなど、契約期間、契約内容に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャネルに番組を可能とするというものである。
【０００６】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する観点からも正当な視聴者のみに（契約チャネル、契約期間に即して）しかも確実に提供する必要がある。
【０００７】これを実現するため、従来は放送受信装置毎にマスター鍵を用意し、受信契約している視聴者に対して受信契約しているチャネルのワーク鍵と視聴可能なチャネル情報などを含む契約形態を示した契約情報をマスター鍵で暗号化して放送波で送信していた。ここでワーク鍵はチャネル固有の鍵であり、暗号化されて送られてくる当該チャネルのチャネルキーを復号することができる。チャネルキーはスクランブル（暗号化された）コンテンツをデスクランブル（復号）するのに用いられる。
【０００８】このような限定受信方式では（受信装置毎に設定された）マスター鍵で暗号化されるワーク鍵と契約情報は受信装置固有の限定受信情報であり、（複数の受信装置に共通の）ワーク鍵で暗号化されたチャネルキーは共通の限定受信情報であると言える。
【０００９】従来は、固有の限定受信情報であっても（固有情報を送信するには不適当な）放送波によって送信していた。これは、個別の加入者に対する情報を全ての加入者に送信しているため不必要に送信帯域を専有しているばかりか、加入者が受信したかどうかの情報も得ることができないため、必要な期間繰り返し送信する必要があった。
【００１０】更に、個別の限定受信情報に含まれるワーク鍵は契約期間（通常１ヶ月）毎に設定され、その期間毎に放送局から個別に限定受信情報を送らなくてはならない上に、受信装置が実際に受信したか否かが契約管理センター側に分からないため、一定期間繰り返し送信しなければならかかった。このため現在限定受信情報に占

める個別の限定受信情報の割合が相当に大きくなっている。

【００１１】この問題を解決するために、電話回線などの双方向通信機能を受信装置に持たせ、各受信装置個別の限定受信情報を双方向回線で、チャネルキーなどの共通の限定受信情報を放送波で送信する方法などが考えられる。しかし、現行の放送事業においては（通常放送の受信のためには）双方向回線が必須ではないため、一部の加入者が限定受信のために双方向回線を所有していないなどの理由によって、全ての加入者に対して双方向回線を前提とした前記の方式が使えなくなることになる。更に、脱着可能な携帯電話などを双方向回線として利用している場合は、限定受信情報送信時に（何らかの事情で）接続されていないため送信できないという問題がある。

【００１２】一方、限定受信情報を双方向回線で送信する際、現在は契約管理センターから受信装置を発呼している。これは受信装置から発呼することにより、発呼の時期が重なって回線が混乱することを避けるためである。しかし、このためセンター側は常に発呼していなければならず、通信費が掛かるという問題がある。更にモバイル受信装置のように携帯電話を双方向回線として利用する場合、（センターからいつ発呼があるか分からないので、）携帯電話を常に着信待ち状態にしておかなくてはならないため電源の消費量が多いという問題がある。

【００１３】

【発明が解決しょうとする課題】このように、従来の限定受信システムは、加入者の増加に伴い各加入者宛に配信すべき情報が増大し、それらを放送配信したのでは、放送帯域が圧迫されてしまうという問題点があった。

【００１４】また、各加入者宛に電話網等の双方向通信にて配信するにしても受信側がそのような受信手段を持たない、あるいは、受信側が電源オフであった場合等通信回線の接続が行えない、あるいは、頻繁に発呼を行う必要があるため送信側の通信費の負担が大きくなる、あるいは、受信側ではいつでも着信待ち状態にしておく必要があるため電力消費量が多くなり、モバイル環境に適していないという問題点があった。

【００１５】そこで、本発明は、このような現状に鑑み、加入者が増加しても放送帯域を圧迫することなく、不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする情報配信方法およびそれを用いた情報配信装置および放送受信装置を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の情報配信方法及び装置は、放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって前記コンテンツ情報の復号のために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記鍵情報を放送配信し、前記受信装置に記憶されている前記復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置との双方向通信により配信し、その際、該受信装置での前記個別制御情報の受領が確認されなかったとき該個別制御情報を放送配信することを特徴とする。

【００１７】本発明によれば、全ての受信装置に共通の鍵情報を放送にて、各受信装置個別の個別制御情報を電話回線等の双方向通信によって配信し、この個別制御情報の受領が確認できなかったときに該個別制御情報を放送配信するので、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。また、個別制御情報を電話回線等の双方向通信により配信することも、放送波で配信することもできるため、視聴するチャネルの変更等を行った時（契約更新時）、受信装置に格納されている復号制御情報（例えば、チャネル契約情報、ワーク鍵等）を更新する際に、双方向通信回線に接続されている受信装置に関しては確実な双方向通信で個別制御情報を送信し、何らかの事情で接続されていない場合には放送波で個別制御情報を送信することができる。すなわち、加入者に確実に個別制御情報を配信することができる。

【００１８】好ましくは、前記受信装置を着信待ち状態にするためのコマンドを放送配信してから前記受信装置を発呼して前記個別制御情報を前記双方向通信により配信することにより、個別制御情報を配信するときのみ、その受信装置を着信待ち状態にするので、受信装置の省電力化が図れるとともに、個別制御情報を確実に配信でき、モバイル環境に適した有料放送システムを提供できる。

【００１９】また、好ましくは、前記個別制御情報を前記双方向通信により配信するために前記受信装置からの発呼を指示するコマンドを放送配信することにより、受信装置側からの発呼によりに個別制御情報を配信する場合であっても、発呼の発生タイミングを情報配信装置側で管理することによって、例えば、受信装置からの発呼がある時間帯に集中することによって、情報配信装置に回線がつながりにくくなるような状況を回避することができる。

【００２０】また、好ましくは、前記受信装置を認証してから前記個別制御情報を双方向通信により配信することにより、特に、受信装置側からの発呼によりに個別制御情報を配信する場合であっても、安全に個別制御情報の配信が可能となる。

【００２１】また、前記鍵情報を前記受信装置に放送配信される鍵生成情報に基づき生成される他の鍵情報で復

号可能なように暗号化して放送配信することによっても上記同様の効果がある。

【００２２】本発明の放送受信装置は、放送配信された暗号化されたコンテンツ情報を受信して、復号すべきコンテンツ情報の復号を行う放送受信装置において、前記放送配信されたコンテンツ情報の復号のために必要な自装置に固有の情報を含む復号制御情報を記憶する記憶手段と、この記憶手段に記憶された復号制御情報の一部または全部を更新するための個別制御情報を配信する第１の配信装置から双方向通信によって配信され、あるいは前記第１の配信装置から放送配信された自装置宛の個別制御情報を受信する第１の受信手段と、この第１の受信手段で双方向通信により自装置宛の個別制御情報を受信したとき、その受領を前記第１の配信装置に送信する受領送信手段と、この第１の受信手段で受信された個別制御情報に基づき前記記憶手段に記憶された復号制御情報を更新する更新手段と、前記コンテンツ情報を復号するために必要な全ての前記放送受信装置に共通の鍵情報を配信する第２の配信装置から放送配信された前記鍵情報を受信する第２の受信手段と、前記記憶手段に記憶された復号制御情報と前記第２の受信手段で受信された鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行うことを特徴とする。

【００２３】本発明によれば、各放送受信装置は、全ての受信装置に共通の鍵情報を放送にて、各受信装置個別の個別制御情報を電話回線等の双方向通信にて、あるいは双方向通信して受信できないときは放送にて受信することにより、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。また、個別制御情報を電話回線等の双方向通信により配信することも、放送波で配信することもできるため、視聴するチャネルの変更等を行った時（契約更新時）、受信装置に格納されている復号制御情報（例えば、チャネル契約情報、ワーク鍵等）を更新する際に、双方向通信回線に接続されている受信装置は双方向通信で個別制御情報を受信し、何らかの事情で接続されていない場合には放送波で個別制御情報を受信することができる。すなわち、各受信装置は確実に個別制御情報を受信することができる。

【００２４】好ましくは、放送配信されたコマンドを受信して、前記第１の配信装置から配信される前記個別制御情報を受信可能なように自装置を着信待ち状態にすることにより、個別制御情報を受信するときのみ、着信待ち状態にすればよいので、受信装置の省電力化が図れるとともに、個別制御情報を確実に配信でき、モバイル環境に適した受信装置を提供できる。

【００２５】また、好ましくは、放送配信されたコマンドを受信して、前記個別制御情報を受信するために前記第１の配信装置を発呼することにより、受信装置側からの発呼によりに個別制御情報を受信する場合であっても、発呼の発生タイミングを情第１の配信装置側で管理することによって、例えば、受信装置からの発呼がある時間帯に集中することによって、センタ（第１の配信装置）に回線がつながりにくくなるような状況を回避することができる。

【００２６】また、好ましくは、自装置が前記第１の配信装置から認証された後、前記個別制御情報を受信することにより、特に、受信装置側からの発呼によりに個別制御情報を受信する場合であっても、安全に個別制御情報の配信が可能となる。

【００２７】また、前記鍵情報は、別途受信した鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化されていることによっても上記同様の効果がある。

【００２８】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

【００２９】まず、用語の定義を行う。１つまたは複数のチャネルからなる放送コンテンツの受信に際し、暗号化などを施して所定の契約・加入手続きなどを行った限られた者（以下、正規の契約者あるいは加入者あるいはユーザと呼ぶ）だけに放送コンテンツの視聴を許可することを総称して限定受信という。また、限定受信を実現するシステムを総称して限定受信システムという。本実施形態では、例えば、有料放送サービスのための限定受信システムを例にとり説明する。

【００３０】限定受信を行なうため各加入者毎にチャネル毎の契約状態を記述した情報をチャネル契約情報と呼ぶ。例えば各チャネルにチャネル番号を付け、図２のようにチャネル番号に対応したビットが「１」であるか否かによりチャネルの契約状態を表したビット列がチャネル契約情報である。図２では第２、第５、第７、第８チャネルが契約されていることを示している。

【００３１】更に、図６に示すように、図２に示したチャネル契約情報に当該チャネル契約情報の有効期限などチャネル契約情報に制限を加える情報や、加入者の契約形態をより詳細に表現する情報を付加してチャンネル契約情報が構成されていてもよい。

【００３２】本実施形態に係る有料放送サービスの各加入者は、それぞれ契約内容（視聴したいチャネルや視聴する期間など）が異なる。すなわち、これら加入者の所持する放送受信装置への限定受信を可能にするためには、各加入者毎に異なる契約内容（利用条件）に基づく当該放送受信装置の制御情報を個別に配信する必要がある。このような制御情報を個別制御情報と呼ぶ。なお、個別制御情報は、パケット形式で配信されるため、その場合は、個別制御パケットとも呼ぶ。この個別制御パケットは、例えば、現行ＣＳ放送規格におけるＥＭＭ（Entitlement Management Message）、ＥＭＭ－Ｓ（Enti

tlement Management Message for S－band）に当たる（参考文献「BSデジタル放送限定受信方式 標準規格 ARIB STD－B25（電波産業会）」）。

【0033】放送コンテンツ情報（以下、簡単にコンテンツと呼ぶことがある）は、各チャンネル毎に異なった鍵情報、すなわち、ここでは「チャネルキー」で暗号化されている。よって、各加入者の所持する放送受信装置にて所望の（契約した）チャネルのコンテンツを視聴するためには、このコンテンツ情報に依存する鍵情報のような全ての加入者（加入者の所持する全ての放送受信装置）に共通の制御情報も配信する必要がある。このような制御情報を共通制御情報と呼ぶ。なお、共通制御情報も、パケット形式で配信されるため、その場合は、共通制御パケットとも呼ぶ。この共通制御パケットは、例えば、現行CS放送規格におけるECM（Entitlement Control Message）、ECM－S（Entitlement Control Message for S－band）に当たる（参考文献「BSデジタル放送限定受信方式 標準規格 ARIB STD－B25（電波産業会）」。

【0034】各加入者の所持する放送受信装置は、個別制御情報と共通制御情報とを確実に受信することにより、各加入者の契約内容に沿ったコンテンツ情報の視聴が可能になるわけである。

【0035】以下の実施形態を通じて、受信装置内部で限定受信方法を実現する構成（主にハードウェア）を限定受信部あるいは限定受信チップという。限定受信チップには限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができない耐タンパ構造を仮定している。また、限定受信部をセットトップボックスとして、このセットトップボックスに、当該セットトップボックスにて復号された音声、映像等のコンテンツ情報を実際に再生するためのテレビ受像器、ラジオ等を接続して、全体として放送受信装置を構成してもよい。

【0036】なお、以下の説明において、暗号化されたコンテンツ情報をチャネルキーを用いて復号することをデスクランブルと呼ぶこともある。

【0037】さらに、以下の実施形態で説明する限定受信システムは、主に、サービス加入者の所持する放送受信装置と、この放送受信装置に個別制御情報、共通制御情報、暗号化コンテンツ情報等を配信する契約管理センター（簡単にセンターと呼ぶことがある）としての情報配信装置（契約管理装置）とから構成される。

【0038】（第1の実施形態）本発明の第1の実施形態は、各受信装置が個別のマスター鍵を有する限定受信システムでの実施形態である。このような限定受信システムは、定期的にしかも個別にチャネル契約情報等を含む制御情報を暗号化して送信しなければならないので送信量が大きくなるという問題点がある。だがその反面マスター鍵が破られた際の被害範囲が狭いなど、安全性が高いため従来からCS放送その他で採用されてきた。しかし、近年の加入者の増加に伴って、受信装置個別に送付すべき制御情報の量が膨大になってきており、本実施形態はこの解決策を与えるものである。

【0039】このような限定受信システムでは、例えば、図3に示すような鍵構成を採用している。即ちチャネル毎に定められている全ての受信装置に共通のワーク鍵Kwを各受信装置個別のマスター鍵KMで暗号化して送信する。更に、そのワーク鍵Kwを使ってチャネルキーKchを暗号化して送信する。放送コンテンツはチャネルキーKchを使って慣用暗号方式で暗号化されているので、このチャネルキーで復号できる。ここでチャネルキーは解読を防ぐため通常10分程度の短時間で変更しなくてはならない。これを送信するために個別のマスター鍵を使っていたのでは送信量が膨大となる。そのため全受信装置に共通のワーク鍵を使う必要がある。またワーク鍵も何ヵ月という単位で同じ鍵を使うと危険なので、変更する必要があり、これを個別のマスター鍵で暗号化する仕組みとなっている。このことにより、例えマスター鍵が知られても、ワーク鍵を変更することによって無料視聴を防止することができる。

【0040】さて、第1の実施形態の限定受信システムに用いられる放送受信装置が放送波から受信するデータはコンテンツパケット、共通制御パケット、個別制御パケットの3種類である。

【0041】コンテンツパケットは図4に示すパケット形式で、情報識別子、チャネル識別子、チャネルキー識別子、スクランブルされた（暗号化された）放送コンテンツからなっている。情報識別子は当該パケットの種別を示すもので、ここではコンテンツパケットであることを示す識別子を記述する。チャネル識別子は当該放送コンテンツがどのチャネルのコンテンツかを示すものである。また、チャネルキー識別子は当該放送コンテンツを復号するチャネルキーの識別子を示す。放送コンテンツは生の番組データで、チャネルキー識別子で指定されたチャネルキーKchで暗号化されている。尚、本実施形態で述べられる全ての情報（データ）は固定長で表現されているものとする。

【0042】ここで説明する共通制御パケットはチャネルキー配信用の共通制御パケットであり、図8に示すパケット形式で、情報識別子、ワーク鍵識別子、チャネル識別子、チャネルキー識別子（1）、チャネルキー（1）、チャネルキー識別子（2）、チャネルキー（2）で構成されており、チャネル識別子からチャネルキー（2）までの部分はワーク鍵識別子で示されたワーク鍵で暗号化されている。情報識別子は当該パケットの種別を示すもので、ここでは共通制御パケット（チャネルキー配信用の共通制御パケット）であることを示す識別子を記述する。チャネル識別子は当該共通制御パケットがどのチャネルものかを示すものである。また、ワー

ク鍵識別子は当該共通制御パケットがどのワーク鍵Ｋｗによって暗号化されているかを示す情報である。チャネルキー識別子は次に記述されているチャネルキーの識別子であり、チャネルキーはチャネル識別子で指定されているチャネルの放送コンテンツの暗号化に使われているチャネルキーを示している。

【００４３】ここで、チャネルキー識別子とチャネルキーが２組存在するのは、前記のようにチャネルキーは比較的短時間で変更されるため、チャネルキーの切り替えをスムーズに行う必要から現在使っているチャネルキーと次回使うチャネルキーを同時に送っているからである。もちろん、このように２組送信することは本発明には直接影響しないので、１組であっても構わない。

【００４４】本実施形態において、個別制御情報は公衆網（電話網）等を用いた双方向通信回線からモデムを経由して配信される場合と放送波によって配信される場合の２通りある。いずれにせよ個別制御情報も共通制御情報と同様にパケット形式で送信されことに変わりはないが、その形式に若干違いがある。

【００４５】双方向通信回線で送信される個別制御パケットは、図７（ａ）に示すような構成の契約情報配信用の個別制御パケットであり、情報識別子、マスター鍵識別子、暗号化された契約情報からなっている。情報識別子は当該パケットの種別を示すもので、ここでは契約情報配信用の個別制御パケットであることを示す識別子を記述する。マスター鍵識別子は当該個別制御パケットを復号できるマスター鍵の識別情報であり、正しく送受信されていれば、ここには当該パケットを受信すべき受信装置の有するマスター鍵識別子が記述されている。

【００４６】放送配信される個別制御パケットは、同じく契約情報配信用の個別制御パケットであり、図７（ｂ）に示すように、未暗号化部分に受信装置ＩＤが付加される点が双方向通信で送信される個別制御パケット（図７（ａ）参照）と異なる。この受信装置ＩＤは当該個別制御パケットがどの受信装置宛てのものであるかを示す情報で、（本パケットを復号する）マスター鍵が受信装置毎で異なるため、不可欠な情報である。

【００４７】契約情報とは、図５に示すように、受信装置ＩＤ、チャネル契約情報、ワーク鍵の数ｎ及びｎ個のワーク鍵とワーク鍵識別子のペア、デジタル署名からなっている。受信装置ＩＤは当該契約情報を受信するべき受信装置の識別子であり、正常に送受信されていれば受信装置内部の限定受信部１００内にある受信装置ＩＤと一致したＩＤである。チャネル契約情報は当該受信装置ＩＤを有する受信装置が受信できるチャネルを示すもので、ここでは、例えば、図６に示すようにチャネル契約情報とその有効期限からなっている。ワーク鍵識別子（ｉ）は続くワーク鍵（ｉ）の識別子である。本実施形態においてワーク鍵はチャネル毎に設定されているため、チャネル契約情報に対応したワーク鍵とワーク鍵識別子の組が入る。デジタル署名は当該契約情報（特にチャネル契約情報）の正当性を確認するための情報であり、主に偽造防止のために用いる。

【００４８】尚、第１の実施形態では、これら全ての情報は固定長で表現されたデータであるので、受信されたパケットから各情報を抽出するアルゴリズムは改めて述べない。

【００４９】次に、第１の実施形態に係る放送受信装置（以下、簡単に受信装置と呼ぶことがある）の構成とその処理動作について説明する。図１は、放送受信装置の要部の構成例を示したもので、まず、図１を参照しながら図９に示す双方向通信による個別制御パケット受信処理動作について説明する。

【００５０】図１の放送受信装置は、モデム部１０１を介し、センターからの発呼に対し応答することで、その双方向通信回線経由で個別制御パケットを送受信するためのセッションが確立される（ステップＳ１）。送受信部１０２は、図７（ａ）に示したような個別制御パケットを受信したとき、その情報識別子から当該パケットが契約情報配信用のものであることを認識したら、それを個別制御情報復号部１０４へ渡し、ここで、当該パケットからマスター鍵識別子を取得する（ステップＳ２、ステップＳ３）。取得したマスター鍵識別子がマスター鍵格納部１０３に格納されているマスター鍵に対応したマスター鍵識別子でなければ、確立されているセッションを利用して、センターへエラーを送信する（ステップＳ３、ステップＳ１０）。対応したマスター鍵識別子であるとき（ステップＳ３）、マスター鍵格納部１０３から出力された当該マスター鍵を用いて（ステップＳ４）、受信したパケットに含まれる契約情報を復号する（ステップＳ５）。

【００５１】復号された契約情報に含まれていたワーク鍵とその識別子をワーク鍵格納部１０５に格納する（ステップＳ１１）。また、当該契約情報に含まれていた受信装置ＩＤと受信装置ＩＤ格納部１０６に格納されている受信装置ＩＤとを比較し、一致しなければ送受信部１０２を介してセンターへエラーを出力する（ステップＳ６、ステップＳ１２）。一致していれば、契約情報認証部１０７でデジタル署名検証鍵格納部１０８に格納されている鍵情報を用いて（例えば、チャネル契約情報あるいは、図５に示す契約情報のうちデジタル署名以外の部分を当該鍵情報で暗号化して、その結果と契約情報中のデジタル署名とを照合することにより）当該契約情報のデジタル署名を検証し（ステップＳ７）、検証が成功しなければ、その旨を送受信部１０２を介してセンターへエラー返信する（ステップＳ１３）。

【００５２】検証が成功すればチャネル契約情報を契約情報格納部１２１に格納した後（ステップＳ８）、センターへ契約情報の更新が正常終了したことを示す受領通知を送信して終了する（ステップＳ９）。

【００５３】ここで契約情報認証部１０７におけるデジタル署名の検証処理について説明する。ここでいうデジタル署名は大きく分けて２つ考えられる。１つは共通鍵暗号を用いたそれであり、センターと受信装置で共通の暗号アルゴリズムと共通の秘密鍵を持ち、契約情報を当該の秘密鍵でブロック単位で逐次的に暗号化し、最後のブロックをデジタル署名とする方式である。ここで逐次的な暗号化とは前のブロックが現在のブロックの暗号化に影響を与えるような暗号化の方式である。例えば、現在のブロックを秘密鍵で暗号化し、その暗号化結果と前のブロックの暗号化結果の排他的論理和をもって現在のブロックの暗号化結果とすることによって実現できる。この方法を使うと、途中のブロックを改竄した場合でも、（ほとんどの場合）異なるデジタル署名が生成されるので改竄検出になる。

【００５４】共通鍵暗号による署名検証は高速に行えるばかり　また、デジタル署名には、前記手法以外にもハッシュ値と呼ばれる署名したいデータ全体の特徴量を計算して、その値を暗号化する手法が知られている。ハッシュ値はデータ全体から計算され、データが１ビットでも変更されるとハッシュ値は著しく異なるばかりか、同じハッシュ値をもつデータを作成することが困難であるという特徴がある。このような性質のため、改竄検出が可能となる。尚、ハッシュ値は固定長データでハッシュ関数で作成される。

【００５５】でなく、回路規模が小さくてすむが、センターと同じ情報を受信装置が持つため、ハッキング等に弱いという特徴がある。

【００５６】もう１つは公開鍵暗号を用いた方法で、秘密鍵で署名したものを公開鍵で検証する。ここで、公開鍵から秘密鍵を導出することが極めて困難なため、受信装置をハッキングして公開鍵を抽出しても、改竄が相当に困難であることが特徴である。極めて安全性の高い方式であるが、低速であるばかりか、回路規模が大きくなるという弱点もある。

【００５７】このようなデジタル署名の優れた性質により、受信装置は（個別制御パケットに付加されたデジタル署名を通じて、）情報配信装置（契約管理装置ともいう）認証しているとも言える。しかし、本発明で考える問題点を解決するためにはデジタル署名は必須ではない。すなわち、本発明の個別制御パケットにおいてデジタル署名は必須ではなく、個別制御パケットからデジタル署名を除いた構成でも矛盾なく本発明を実施できる。

【００５８】次に、図１０～図１４に示すフローチャートを参照して、図１の放送受信装置が放送波から共通制御情報とコンテンツ情報と共通制御情報を受信する処理動作について説明する。受信装置はセンターから発信された放送波を放送受信部１１１で受信して電気信号を得ると（ステップＳ２１）、それをＡ／Ｄ変換部１１２でアナログ信号からデジタル信号に変換してパケット形式のデジタルデータに変換する（ステップＳ２２、ステップＳ２３）。デジタルデータは誤り検出／訂正部１１３に送られ所定の誤り検出／訂正が行われた後（ステップＳ２４）、当該受信パケットの情報識別子を参照してコンテンツパケット、共通制御パケット、個別制御パケットのいずれかを判別して、それに従って分岐して処理を進める。

【００５９】ところで、チャネル選択インタフェース（Ｉ／Ｆ）１１５は、現在視聴中のチャネル識別子を取得するもので、ここで取得されたチャネル識別子はチャネル選択部１１４とチャネル情報入力部１２３へ渡される（図１２のステップＳ５１～ステップＳ５３）。

【００６０】コンテンツパケットである場合は（ステップＳ２５）、チャネル選択部１１４は、現在視聴中のチャネルをチャネルＩ／Ｆ１１５を介して得て、これを基に、視聴チャネルのコンテンツパケットのみ限定受信部１００のフィルター部１１６に渡す（ステップＳ２８）。フィルター部１１６では、これをデスクランブル部１２０へ送る（ステップＳ２９）。

【００６１】一方、共通制御パケットである場合は（ステップＳ２６）、チャネル選択部１１４を経て、フィルター部１１６で共通制御情報復号部１１７へ送られ、復号が開始される（ステップＳ４１）。

【００６２】次に、コンテンツパケットに対する処理を図１１のフローチャートに沿って詳しく説明する。図１０のステップＳ２９でデスクランブル部１２０へ送られたコンテンツパケットからチャネル識別子とチャネルキー識別子とがを分離され、それらがチャネルキー出力部１１９に渡される。デスクランブル部１２０からチャネルキー出力部１１９に対してチャネルキーの出力を要請する。

【００６３】チャネルキー出力部１１９は、契約判定部１１２での当該チャネル識別子に対する契約判定を基に現在視聴中の受信チャネルのチャネルキーをチャネルキー格納部１１８から抽出する。すなわち、図１２に示すように、契約判定部１２２は、チャネル情報入力部１２３から現在視聴されているチャネルのチャネル識別子を取得し（ステップＳ５４）、契約情報格納部１２１にすでに記憶されている図２に示したようなチャネル契約情報を参照して、取得したチャネル識別子に対応するビットが「１」であれば「許可」、「０」であれば「不許可」の信号をチャネルキー出力部１１９に送る（ステップＳ５５）。チャネルキー出力部１１９では、送られてきた判定結果が「許可」であればチャネルキー格納部１１８からコンテンツパケットから取り出されたチャネルキー識別子を持つチャネルキーをチャネルキー格納部１１８から得て、デスクランブル部１２０へ渡す（ステップＳ５７）。判定結果が「不許可」であれば、そこで当該コンテンツパケットに関する処理を終了する。

【００６４】デスクランブル部１２０は、チャネルキー

出力部１１９からチャネルキーを受け取ると、それを用いてコンテンツパケットに含まれる暗号化されたコンテンツ情報を復号して出力する（図１１のステップＳ３１～ステップＳ３３）。

【００６５】次に、共通制御パケットに対する処理を図１３に示すフローチャートを参照して説明する。共通制御パケットはフィルター部１１６から共通制御情報復号部１１７に送られる（図１０のステップＳ４１）。ここで、共通制御パケットの未暗号部に含まれるワーク鍵識別子を基にワーク鍵格納部１０５からワーク鍵を取得する（図１３のステップＳ４２）。ワーク鍵が取得できなかった場合、処理を終了する。ワーク鍵が取得できたら、当該ワーク鍵で共通制御パケットの暗号化部を復号する（ステップＳ４４）。復号された共通制御パケットの暗号化部からチャネルキーＫｃｈを取得し、チャネルキー格納部１１８に格納する（ステップＳ４５）。

【００６６】次に、個別制御パケットに対する処理について図１４に示すフローチャートを参照して説明する。個別制御パケットはフィルター部１１６から個別制御情報復号部１０４に送られる（図１０のステップＳ６１）。ここで、個別制御パケット（の未暗号化部）から受信装置ＩＤを抽出し、受信装置ＩＤ格納部１０６に格納されている自装置の受信装置ＩＤと照合する（図１４のステップＳ６２）。抽出された受信装置ＩＤが自装置のそれと一致しなかった場合は、本パケットの処理を終了する。一致した場合は当該受信パケット（の未暗号化部）から取り出されたマスター鍵識別子をキーにしてマスター鍵格納部１０３からマスター鍵を取得する。更に、当該マスター鍵を使って当該個別制御パケット中の契約情報を復号し（ステップＳ６３）、復号して得られた契約情報（図５参照）からワーク鍵とその識別子を取り出してワーク鍵格納部１０５に格納する（ステップＳ６４）。

【００６７】次に、復号された契約情報は、契約情報認証部１０７に送られる。契約認証部１０７では、この契約情報のデジタル署名以外の部分をデジタル署名検証鍵格納部１０８に格納されているからデジタル署名検証鍵を用いて暗号化してデジタル署名を取得し、当該契約情報中のデジタル署名と一致しているか否かに基づきデジタル署名を検証する（ステップＳ６５）。検証が成功した場合は契約情報中のチャネル契約情報を契約情報格納部１２１へ格納して処理を終える（ステップＳ６６）。検証が失敗した場合はチャネル契約情報が偽造されたか、受信不良によって壊された可能性があるので格納せずに終了する。

【００６８】以上説明したように、上記第１の実施形態に係る放送受信装置によれば、個別制御情報を電話回線等の双方向通信により受信する場合と、放送波で配信されたものを受信する場合との両方で受信することができるため、視聴するチャネルの変更等を行った時（契約更新時）、受信装置に格納されているチャネル契約情報等を更新する際に、双方向通信回線に接続されている受信装置に関しては確実な双方向通信で個別制御パケットを送信し、何らかの事情で接続されていない場合には放送波で個別制御パケットを送信することができる。

【００６９】第１の実施形態では、放送受信装置の構成のみを示したが（第１の実施形態に係る情報配信装置は、第５の実施形態で説明する）、前述したような個別制御情報を双方向通信と放送との両方で配信することにより、例えば、携帯電話等の双方向通信機能を持たない（図１のモデム部１０１，送受信部１０２を持たない）放送受信装置であっても、チャネル契約情報の更新が確実に行える。

【００７０】（第２の実施形態）次に、いくつかのバリエーションを述べる。第１のバリエーションは個別制御情報をセンターから双方向通信回線を用いて送信するに先だって、受信装置側の双方向通信機能（例えば携帯電話機能）の電源をオンにする命令を放送波で送信するものである。

【００７１】このようにすることによって受信装置側はいつ着信するか分からない個別制御情報のために常時電源オン状態（着信待ち状態）にする必要がなくなり、省電力が実現できる。このような省電力の実現は電池を主な電源とするモバイル環境においては重要である。

【００７２】第２の実施形態に係る放送受信装置の要部の構成を図１５に示すが、図１５において、双方向通信機能とは、送受信部１０２、モデム部１０１以降に対応するが、本発明は、限定受信部に特徴があるので、双方向通信機能部の詳細構成とその説明は省略し、その機能の電源オン／オフ制御を行う動作に係る構成のみ説明する。例えば、送受信部１０２に所定の接続ケーブルを用いて携帯電話を接続して双方向通信機能部を構成することもできる。

【００７３】図１５において、放送波で送信する個別制御パケットの受信処理に関する構成部が第１の実施形態と異なっている。実際、共通制御パケットの受信手順は第１の実施形態と同じであるので、以下では異なっている点、すなわち、放送波から受信する個別制御パケットの構成とその受信処理動作のみを説明するに留める。

【００７４】第２の実施形態において、放送波で受信される個別制御パケットは、契約情報配信用のものと、コマンド配信用のものとの２種類である。契約情報配信用の個別制御パケットは第１の実施形態のもの（図７（ｂ）参照）と同じであるので、ここではコマンド配信用の個別制御パケット（以下、コマンドパケットと呼ぶことがある）のみを説明する。

【００７５】コマンドパケットは図１６に示すように、情報識別子とコマンド本体からなっている。コマンド本体は、大きく分けて図１７に示すように、コマンド識別子と受信装置ＩＤの数とその受信装置ＩＤの数だけ受信

装置ＩＤが並び、その後にデジタル署名が続く。デジタル署名は受信装置ＩＤの数と受信装置ＩＤの並びに対して偽造防止のために付けられる。ここでのコマンド識別子は、いつでも着呼可能な状態に（着信待ち状態）にするための例えば、放送受信装置の双方向通信機能への電源の供給を開始するための「電源オン」コマンドであることを識別するためのコマンド識別子である。以下、「電源オン」コマンドを配信するコマンドパケットを電源オンコマンドパケットと呼ぶ。

【００７６】図１８は、図１５に示した放送受信装置の放送波による個別制御パケットの受信処理動作を説明するためのフローチャートである。以下、図１５に基き、図１８に沿って処理の流れを説明する。

【００７７】まず、フィルター部１１６から個別制御情報復号部１０４にパケットが渡される。当該パケットの情報識別子を参照し、当該パケットが契約情報配信用の個別制御パケットであった場合は、第１の実施形態の場合（図１４参照）と同様の処理を行う（ステップＳ７１～ステップＳ７６）。

【００７８】個別制御情報復号部１０４では、当該パケットがコマンドパケットであった場合、パケット内のコマンド識別子を参照して、当該パケットが電源オンコマンドパケットであるか否かチェックする（ステップＳ７７）。当該パケットが電源オンコマンドパケットでなければ処理を終了する。

【００７９】電源オンコマンドパケットであった場合、受信装置ＩＤ格納部１０６に格納されている自装置の受信装置ＩＤと当該パケット内の受信装置ＩＤとを１つずつ照合する（ステップＳ７８）。ここで自装置の受信装置ＩＤがパケット内に含まれていなかった場合、処理を終了する。含まれていた場合は、当該パケットを個別制御情報認証部１０７に送る。

【００８０】個別制御情報認証部１０７では、デジタル署名検証鍵格納部１０８から検証鍵を取得して、デジタル署名を検証する（ステップＳ７９）。デジタル署名の検証が失敗した場合は処理を終了し、成功した場合は電源管理部１２５にモデム部１０１、送受信部１０２等の双方向通信機能に係る機能部への電力供給を開始する（電源オンにする）旨の信号を送り、電源管理部１２５はそれを受けて、これら機能部への電力の供給を開始して、いつでも着信待ち状態にする（ステップＳ８０）。

【００８１】ステップＳ８０で双方向通信機能が着信待ち状態となるので、その後、図９に示したような手順にて、放送受信装置は契約情報配信用の個別制御パケットを双方向通信回線を介して受信することができる。

【００８２】なお、ここで言う電源とは双方向通信回線の着信待ちのための待機電源（電力）を意味しているが、構成によってはその他の構成部の電源オン（もしくはオフ）が当該コマンドパケットにより可能となる。尚、電源管理部１２５は、本実施形態でオンになった電源を契約情報配信用の個別制御パケットを双方向通信回線を介して受信した後もしくは受信しなくても一定期間の後にオフすることが望ましい。

【００８３】このように個別制御パケットを放送波と通信に分けて送信することによって、帯域削減及び省電力という意味で有効な限定受信システムを構成することができる。以上で第１のバリエーションの説明を終わる。

【００８４】（第３の実施形態）第１の実施形態の第２のバリエーションについて説明する。個別制御情報をセンターから双方向通信回線を使って送信するために、放送受信装置側から発呼を行う方式に関するバリエーションである。受信装置側から発呼を行うと発呼が一様に分布しないためセンター側システムで受信できない場合がある。本実施形態は、この問題点を解決しようとするものである。更に、本実施形態においては、発呼している受信装置が正当なものか否かを認証する手段を設けている。発呼を一様にするという目的には認証は必ずしも必要ではないが、第１～第２の実施形態のようなセンター発呼と異なり受信装置発呼の場合は受信装置の正当性が認証しにくく、認証手段を持たないと安全性を保ちにくい。

【００８５】第３の実施形態に係る放送受信装置の要部の構成を図１９に示す。図１９において、放送波で配信される個別制御パケットを受信する処理動作が第１の実施形態の場合と異なる。従って、以下では放送波から受信する個別制御パケットの構成とその受信処理動作についてのみを説明するに留める。

【００８６】第３の実施形態では第２の実施形態と同様、放送波で受信される個別制御パケットは、契約情報配信用とコマンド配信用（コマンドパケット）の２種類である。契約情報配信用の個別制御パケットのデータ構成は第１の実施形態で説明したものと同様であり（図７（ｂ）参照）、コマンドパケットの構成も第２の実施形態で説明したもの（図１６、図１７参照）と同様であるが、本実施形態では、コマンド識別子が放送受信装置に対しセンターへの発呼を指示するコマンドの識別子である点が異なる。以下、このようなコマンドを発呼コマンドと呼び、そのパケットを発呼コマンドパケットと呼ぶ。

【００８７】図２０は、図１９の放送受信装置の放送波による個別制御パケットの受信処理動作を説明するためのフローチャートで、以下では、図１９に基き、図２０に沿って処理の流れを説明する。

【００８８】まず、フィルター部１１６から個別制御情報復号部１０４に放送波により受信された個別制御パケットが渡される。当該パケットの情報識別子を参照し、当該パケットは契約情報配信用のパケットであった場合は、第１の実施形態と同様の処理（図１４参照）を行う（ステップＳ９１～ステップＳ９６）。

【００８９】当該パケットがコマンドパケットであった

場合、パケット内のコマンド識別子を参照して、当該パケットが発呼コマンドパケットであるか否かチェックする（ステップＳ９７）。当該パケットが発呼コマンドパケットでなければ処理を終了する。

【００９０】発呼コマンドパケットであった場合、受信装置ＩＤ格納部１０６に格納されている自装置の受信装置ＩＤと当該パケット内の受信装置ＩＤとを１つずつ照合する（ステップＳ９８）。ここで自装置の受信装置ＩＤがパケット内に含まれていなかった場合、処理を終了する。含まれていた場合は当該パケットを個別制御情報認証部１０７に送る。

【００９１】個別制御情報認証部１０７では、デジタル署名検証鍵格納部１０８から検証鍵を取得して、デジタル署名を認証する（ステップＳ９９）。デジタル署名の検証が失敗した場合は処理を終了し、成功した場合はセンター発呼部１６２にセンターへの発呼を指示する旨の信号を送り、センター発呼部１６２はセンター間通信部１５２、モデム部１０１を通してセンターへの発呼を行う（ステップＳ１００）。

【００９２】このように、個別制御パケットを放送波と双方向通信との両方を用いて送信する限定受信システムにおいて、受信装置側からの発呼により当該受信装置とセンター間の双方向通信回線の接続を行う場合、受信装置からの発呼をセンター側から指示して行わせ、発呼の発生タイミングをセンター側で管理することによって、例えば、受信装置からの発呼がある時間帯に集中することによって、センタに回線がつながりにくくなるような状況を回避することができる。

【００９３】次に、放送受信装置がセンターに対し発呼を行ってから、個別制御パケットを受信するまで処理動作について説明する。センターと放送受信装置との間の双方向通信で送受信されるパケットは、図２１に示すように、情報識別子と情報本体からなっている。この情報本体の違いにより３つのパケットに分類できる。ここでは、例えば、図７（ａ）に示した個別制御パケットと同様のパケット（以下、このパケットを、他の２種類のパケットを区別するためにあえて個別制御パケットと呼ぶ）とチャレンジパケットとレスポンスパケットとがある。

【００９４】個別制御パケットは、図２２に示すように情報識別子、マスター鍵識別子、暗号化された契約情報からなっている。ここで契約情報は、図５と同様である。チャレンジパケットは、図２３に示すように、チャレンジパケットであることを識別するための情報識別子と、チャレンジ番号とチャレンジ情報本体からなっており、チャレンジ番号とはチャレンジと呼ばれるセンターから受信装置への質問や問題の管理番号である。本実施形態で想定しているチャレンジは、受信装置ＩＤを問い合わせるチャレンジ、マスター鍵識別子を問い合わせるチャレンジ、チャレンジ情報に（各受信装置固有の）秘密鍵で署名を作成するチャレンジである。この他にも、暗号化されたチャレンジ情報を秘密鍵で復号させ、復号結果をレスポンスさせるチャレンジなども考えられる。ここで秘密鍵で署名させるチャレンジのように対象データが必要な場合、それをチャレンジ情報本体に記述して送信する。

【００９５】チャレンジアンドレスポンスの基本は放送受信装置とセンターのみしか知り得ない情報を使わないと答えられないように質問をして、その質問に正確に答えられたことで、当該放送受信装置が（センターに登録されている）正当な装置であることを確認することにある。

【００９６】レスポンスパケットは図２４に示すように、レスポンスパケットであることを識別するための情報識別子と、チャレンジ番号とチャレンジ情報本体、レスポンス情報本体からなっている。レスポンス情報本体も（チャレンジ情報本体と同様に）チャレンジ番号によって形式が定まっているものとする。

【００９７】図２５は、受信装置が、発呼コマンドを受けた後の処理動作を示したフローチャートであり、以下、図１９に基き図２５に沿って処理の流れを説明する。まず、受信装置からセンターに対して発呼が行われ（ステップＳ１０１）、双方向通信回線が受信装置とセンター間に接続されると、センターから個別制御パケットが送信される。受信装置のセンター間通信解析部１５１は、当該接続された双方向通信回線、モデム部１０１，センター間通信部１５２を介して個別制御パケットを受信する（ステップＳ１０２）。受信したパケットは、センタ間通信解析部１５１へ渡され、ここで、そのパケットの情報識別子からどの種別のパケットであるかを識別する。

【００９８】センター間通信解析部１５１は、当該受信したパケットがチャレンジパケットである場合（ステップＳ１０３）、レスポンス作成部１５２にそれを渡す（ステップＳ１０６）。契約情報配信用の個別制御パケットであった場合は（ステップＳ１０４）、個別制御情報復号部１０４へ渡して（ステップＳ１０７）、第1の実施形態と同様の処理（図９のステップＳ３～ステップＳ９）によって契約情報の認証と格納処理を行う（ステップＳ１０８）。受信したパケットが上記いずれでもなかった場合はエラーとして双方向通信回線を介してセンターへ送信する（ステップＳ１０５）。

【００９９】次に、レスポンスパケットの作成および送信処理動作について図２６に示すフローチャートに沿って説明する。レスポンス作成部１５２は、チャレンジパケット中のチャレンジ番号を参照して、チャレンジの種別を確認する。受信装置ＩＤの問い合わせるチャレンジであるときは（ステップＳ１１１）、受信装置ＩＤ格納部１０６から受信装置ＩＤを取り出して（ステップＳ１１５）、予め定められたレスポンス情報形式に受信装置

ＩＤを変換して図２３に示すようなレスポンスパケットを作成し（ステップＳ１１６）、センターへ送信する（ステップＳ１１７）。マスター鍵識別子を問い合わせるチャレンジであったとき（ステップＳ１１２）、マスター格納部１０３からマスター鍵識別子を取得して、前述同様にレスポンスパケットを作成し、センターへ送信する（ステップＳ１１８～ステップＳ１２０）。

【０１００】署名作成のチャレンジであった場合は（ステップＳ１１３）、署名すべきデータであるチャレンジ情報本体を受信したパケット中から取得し（ステップＳ１２１）、秘密鍵格納部１５３から秘密鍵を取得して（ステップＳ１２２）チャレンジ情報本体に対する署名を作成する（ステップＳ１２３）。作成された署名は予め定められた形式にしたがってレスポンス情報本体の形式に変換され、図２４に示すようなレスポンスパケットの形式でセンターへ送信される（ステップＳ１２４～ステップＳ１２５）。送信されてきたチャレンジ情報が上記3通りのどれにも当てはまらない場合はエラーをセンターに送信する（ステップＳ１１４）。

【０１０１】以上の処理によって、センター側が、受信したレスポンスパケットから当該受信装置の正当性を確認した上で個別制御パケットを送信することができるのである。尚、（第１の実施形態で述べたように）、本実施形態においては、個別制御パケットに付されたデジタル署名によって受信装置が情報配信装置（センター）側を認識しているとも言える。このため、本実施形態により受信装置とセンターとの間で相互認証が行われていると考えることも可能である。しかし、第１の実施形態でも述べたように、このような形態は、本発明において必須ではなく、本発明のようにセンター側が受信装置を認識する実施形態が本質的である。

【０１０２】以上で第２のバリエーションの説明を終わる。

【０１０３】尚、双方向通信による個別制御パケット送信のための発呼を受信装置、センター相方で行うことができるような限定受信システムにおいては、第２、第３の実施形態を同時に満たすような限定受信方式も実施可能である。何故なら両バリエーションは（その構成から）コマンドの種類（コマンド識別子）が違うだけで、互いに独立な関係にあるので、両方同時に実施することも可能だからである。この意味で第１、第２の実施形態は、各受信装置個別のコマンドパケットを放送で、契約情報配信用の個別制御パケットを双方向通信で送信する実施形態と捉えることができる。

【０１０４】以上の実施形態において主要な処理を限定受信部１００の中だけで行っているが、デスクランブル部１２０のみを限定受信チップの外側で実装するという考え方もある。デスクランブル部１２０は（放送コンテンツを復号するのであるから）リアルタイムに復号しなくてはならないため高速処理が必要である。しかし、その他の部分は常に動作しなくてはならないわけではなく、しかも処理時間に多少の余裕があるため実装上このようにすると有利なことが多い。更に、他の放送との受信装置の共通化を図る際、全ての放送で放送コンテンツのスクランブル方式を共通にして、（各放送で秘密情報を保持したい）限定受信部１００のみをＩＣカードなど脱着可能なメディア上に実装する実装方法が考えられる。以上説明した実施形態、及びこれから述べる実施形態においては前記のような実装も可能であることを付け加えておく。

【０１０５】（第４の実施形態）第４の実施形態は、全ての放送受信装置が共通のマスター鍵を有する限定受信システムの場合である。第４の実施形態における限定受信システムはマスター鍵が全ての放送受信装置で共通であるため、第１の実施形態におけるワーク鍵の役割を（全受信装置に共通の）マスター鍵が果たしているので、図２８に示すように、ワーク鍵が存在しない簡単な鍵構成になっている。このような限定受信システムは構成が単純なため、（放送波での送信を前提にした場合）個別制御情報の送信量削減の点で大変有用である（特開平１１－２４３５３６参照）。しかし、マスター鍵が共通であるため、どの放送受信装置にも等しく全てのチャネルのチャネルキーが受信されてしまうため限定受信を実現するためにはチャネル契約情報のみに依存することになる。

【０１０６】第４の実施形態に係る放送受信装置の要部の構成を図２７に示す。第４の実施形態では第１の実施形態の場合と同様に、図７に示したような個別制御パケットが用いられる。但し、第４の実施形態ではワーク鍵が存在しないので、契約情報は図２９に示すような受信装置ＩＤとチャネル契約情報とデジタル署名とからなる構成を持つ。また、共通制御パケットは、マスター鍵生成情報配信用の共通制御パケット（図３０（ａ）参照）とチャネルキー配信用の共通制御パケット（図３０（ｂ）参照）の２種類が用いられる。

【０１０７】チャネルキー配信用の共通制御パケットは、第１の実施形態の場合（図８参照）と同様である。マスター鍵生成情報配信用の共通制御パケットは、図３０（ａ）に示すように、情報識別子、マスター鍵識別子、マスター鍵生成情報、デジタル署名からなっている。

【０１０８】ここで、情報識別子は当該パケットがマスター鍵生成情報配信用の共通制御パケットであることを示す情報で、他のパケットと区別するために用いられる。マスター鍵識別子は続くマスター鍵生成情報から生成されるマスター鍵の識別子である。デジタル署名は当該マスター鍵生成情報の偽造を防止するためのものであり、第１の実施形態で用いているデジタル署名と同様に秘密鍵暗号によるもの、公開鍵暗号によるものがあり、どちらを使ってもよい。

【0109】次に、図27の放送受信装置の構成とその処理動作について説明する。第4の実施形態に係る放送受信装置の処理動作は第1の実施形態のそれと重なる部分が多いので、異なる部分のみを説明するに留める。

【0110】共通制御パケットの受信処理動作について図31をに示すフローチャートを参照して説明する。図31では、受信装置が共通制御パケットを受信し、共通制御パケットがフィルター部116から共通制御情報復号部117へ渡された時点で開始される。

【0111】まず、共通制御情報復号部117は、当該受信パケットの情報識別子を参照して当該パケットがチャネルキー配信用のものであるか判定する（ステップS301）。チャネルキー配信用の共通制御パケットであれば、当該パケットの未暗号部分からマスター鍵識別子を抽出し、当該マスター鍵識別子を有するマスター鍵をマスター鍵格納部105から取得する（ステップS302）。取得したマスター鍵を使ってパケットの暗号化部を復号する（ステップS303）。復号した結果得られたチャネルキーをチャネルキー格納部118へ格納し、終了する。

【0112】一方、受信したパケットがマスター鍵生成情報配信用の共通制御パケットであれば（ステップS305）、当該パケットからマスター鍵識別子を取り出し、そのマスター鍵識別子に対応したマスター鍵がマスター鍵格納部103に存在するか否かを判定する（ステップS306）。既に存在する場合はそこで終了する。存在しない場合は、次に新しいマスター鍵の生成を行う。

【0113】まず、マスター鍵生成情報検証部181は、当該パケットに含まれるデジタル署名を検証し（ステップS307）、検証失敗した場合は終了、検証成功した場合はマスター鍵生成部182で、当該パケットに含まれるマスター鍵生成情報から予め定められたアルゴリズムに従ってマスター鍵を生成し（ステップS308）、その生成されたマスター鍵をマスター鍵格納部103に格納して終了する（ステップS309）。

【0114】ここで、マスター鍵生成情報とマスター鍵生成処理の説明を少ししなくてはならない。マスター鍵生成情報とは例えばマスター鍵生成のための乱数シード情報であり、乱数シードとマスター鍵生成部182の予め定められたアルゴリズムとパラメータによる乱数生成の手段によりマスター鍵を生成するものである。生成は耐タンパハードウェアの中で行われるため、マスター鍵生成情報は未暗号化のままでも安全上の問題はない。

【0115】また、双方向通信によって送信される個別制御パケットの受信より動作は第1の実施形態と同様である。

【0116】なお、第4の実施形態についても第1の実施形態のバリエーション（第2，第3の実施形態）を適用することが可能である。

【0117】（第5の実施形態）第5の実施形態は第1の実施形態に係る放送受信装置に対し個別制御パケット共通制御パケットを配信するためのセンター側に設けられた情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。

【0118】図32は、第5の実施形態に係る情報配信装置の要部の構成例を示したもので、以下、図32を参照しながら図35～図39に示すフローチャートに沿って図32に示す情報配信装置の構成と処理動作について説明する。

【0119】図32において、加入者データベース（DB）202には、全ての加入者の加入者データが格納されている。加入者データのデータ構成は図33に示すように、加入者ID、受信装置ID、マスター鍵識別子、マスター鍵、チャネル契約情報、送信済みフラグ、放送送信フラグ、発呼番号からなっており、これが一件の加入者データである。

【0120】加入者IDとは各加入者に対して付加された管理番号のことで、本実施形態では簡単のため1番から「MAXID」番までの番号がふられているとする。受信装置IDは加入者IDに示す加入者の受信装置IDを示している。マスター鍵識別子は当該加入者の受信装置の内部（マスター鍵格納部103）に現在存在するマスター鍵の識別子であり、マスター鍵は当該マスター鍵識別子に対応したマスター鍵である。チャネル契約情報は、図2、図6に示すように、当該加入者の契約状態を表すものである。送信済みフラグは当該加入者に当該チャネル契約情報を双方向通信にて送信したか否かを示すフラグであり、「0」の時未送信、「1」の時は送信済みとなる。放送送信フラグは当該加入者データの当該チャネル契約情報を放送配信すべきか否かを示すフラグであり、「0」の時は放送配信する必要がない旨を示し、「1」の時は放送配信する必要がある旨を示している。

【0121】ここでは、個別制御パケットの配信は、まず、双方向通信にて配信するものとし、その際、それを受けるべき受信装置に対し何度も発呼を試みたにも関わらず、正常受信しなかった、エラーが返信されてきた、応答がなかった等の場合には、その個別制御パケットの配信を放送配信に切り替えるものとする。放送受信装置に対する個別制御パケットの配信を双方向通信から放送配信に切り替えるまでに許容される発呼の回数をNとする。また、発呼番号は当該加入者の受信装置に接続されている双方向通信回線の電話番号であるとする。

【0122】まず、図32の情報配信装置における個別制御パケットを双方向通信にて送信する際の処理動作を図35に示すフローチャートに沿って説明する。この処理は、ワーク鍵更新の都度定期的に個別制御情報制御部206によって起動される。

【0123】個別制御パケット作成指示を個別制御情報制御部206から受けた個別制御情報作成部203は、

変数ｋ＝０（ステップＳ３３０１ａ）、ｉ＝１とし（ステップＳ３０１ｂ）、加入者ＩＤがｉである加入者データが加入者ＤＢ２０２内に存在するか否かをチェックする（ステップＳ３０２）。存在しなかった場合の処理を述べる。存在しなかった場合は、ステップＳ３１３に進み、ｉを１つインクリメントし、ｉが「ＭＡＸＩＤ」を越えないことを確認した上で（ステップＳ３１４）、ステップＳ３０２へ戻り、新しいｉで加入者ＩＤをチェックする。

【０１２４】ステップＳ３１４で、ｉが「ＭＡＸＩＤ」を越えてしまったら、全ての加入者データについて一通りの処理が終了したことを意味するので、次に、ステップＳ３１５へ進み、加入者ＤＢ２０２を全検索して、未送信の加入者データが存在するか否か（送信済みフラグが「０」である加入者データがあるか否か）を検査する。ここで未送信の加入者データがあれば、ｋ（加入者ＤＢ３０２内の加入者データのｋ回目のサーチという意味）を１つインクリメントし（ステップＳ３１６）、ｋがＮ（発呼回数の最大値）を越えた場合（ステップＳ３１７）、その時点で加入者データの送信済みフラグが「０」の加入者については、個別制御パケットを双方向通信で配信するのを諦め、送信済みフラグが「０」の全ての加入者の加入者データの放送送信フラグを「１」にして終了する（ステップＳ３１８）。ｋが１を越えなければ、ステップＳ３０１ｂに戻り、ｉ＝１にして以降の処理を繰り返す。ステップＳ３１５において、未送信フラグが「０」の加入者レコードがなければ終了する。ｋがＮを越えなかった場合、ｉ＝１にして本アルゴリズムを最初から行う。また、未送信の加入者データがなければ終了する。

【０１２５】ステップＳ３０２で、加入者ＩＤがｉの加入者データが存在した場合、当該加入者データ中の送信済みフラグを参照して、「１」であれば送信済みなので、ステップＳ３１３へ進み、ｉを１つインクリメントした後、ｉが「ＭＡＸＩＤ」を越えていなければ（ステップＳ３１４）、ステップＳ３０２へ戻り、加入者ＩＤの存在チェックに戻る。尚、この「ＭＡＸＩＤ」を越えるまでｉを１つづインクリメントしながら加入者ＩＤの存在チェックを行う処理は、下でも度々現れる処理であるので、以下の説明では簡単のためインクリメント処理と呼ぶことにする。

【０１２６】ステップＳ３０２で、加入者ＩＤ＝ｉの加入者データが存在した場合、当該加入者データの送信済みフラグを参照して、「１」であれば送信済みなのでｉを１つインクリメントして加入者ＩＤの存在チェックに戻る。送信済みフラグが「０」であった時は、個別制御情報作成部２０３は、当該加入者データのチャネル契約情報に基づいて必要なワーク鍵をワーク鍵ＤＢ２１０から取得する（ステップＳ３０４）。ここでワーク鍵は（第１の実施形態でも説明したように）チャネル毎に設定されていると仮定しているのでこのように契約したチャネル分だけのワーク鍵を取得する処理が必要になる。

【０１２７】個別制御情報作成部２０３は、取得されたワーク鍵と当該加入者データの受信装置ＩＤ、チャネル契約情報からデジタル署名以外の契約情報本体を作成し、デジタル署名生成鍵格納部２０５に格納されているデジタル署名生成鍵を用いて、この契約情報本体あるいは、契約情報本体とその特徴量としてのハッシュ値とを暗号化することでデジタル署名を作成して、図５に示したような契約情報を作成する。更に当該加入者データ中のマスター鍵でこの作成した契約情報を暗号化し、マスター鍵識別子や情報識別子を付加して、図７（ａ）に示したような個別制御パケットを作成する（ステップＳ３０５）。

【０１２８】作成したパケットは、個別制御情報制御部２０６を介して当該加入者データ中の発呼番号とともに、送受信制御部２０７に渡され、送受信制御部２０７は、この発呼番号を用いて当該加入者の図１に示した放送受信装置を発呼する（ステップＳ３０６）。この発呼に対し当該受信装置が応答を返してこなかった場合は（ステップＳ３０７）、エラー出力部２１５から受信エラーを出力して（ステップＳ３０８）、ステップＳ３１３へ進み、インクリメント処理を行って、次の加入者データに処理を移す。

【０１２９】ステップＳ３０７において、発呼に対して当該受信装置から応答が返ってきた場合は、予め定められたプロトコルによって、作成した個別制御パケットを送信する（ステップＳ３０７）。送信後、一定期間に受信装置より受領通知があった場合（ステップＳ３１０）、個別制御情報制御部２０６は、当該加入者データの送信済みフラグを「１」にして（ステップＳ３１２）、ステップＳ３１３へ進みインクリメント処理を行ったのち、次の加入者データに処理を移す。

【０１３０】インクリメント処理の部分でも述べたように本処理は、ｉが「ＭＡＸＩＤ」を越え、全ての加入者データが送信済みであることを確認するか（ステップＳ３１５）、ｋが既定値Ｎを越え、個別制御パケットの双方向通信による配信を諦めた時終了する（ステップＳ３１８）。

【０１３１】次に、図３２の放送により共通制御パケットと個別制御パケットとを送信するための送信処理動作とこの送信処理動作に係る構成部について、図３６に示すフローチャートに沿って説明する。本処理は、放送開始と同時に開始され、放送が続く間間断なく繰り返される。まず、共通制御情報作成部２０９は、チャネルキーデータベース（ＤＢ）２１１を検索して、最小のチャネルＩＤを持つチャネルキーデータを取得する（ステップＳ４０１）。

【０１３２】ここでチャネルキーデータはチャネルキーＤＢ２１１に登録されているチャネル毎の少なくともチ

ャネルキーを含むデータで、図３４に示す構造をしている。チャネルキーデータはチャネルＩＤとチャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）からなっている。ここでチャネルＩＤとは各チャネルにふられるＤＢ管理上の番号である。チャネル識別子は、放送受信装置が各チャネルを識別するための情報で第１～第４の実施形態で説明したそれと同じである。更にチャネルキー識別子及びチャネルキーも第１～第４の実施形態で述べたものと同じである。

【０１３３】ここでチャネルキーとその識別子とのペアが２組存在するのは現在有効なチャネルキー（チャネルキー（１））と次に使われるチャネルキー（チャネルキー（２））を一緒に送信する必要があるためであり、構成によっては現在使用されているチャネルキーのみでも構わない。

【０１３４】まず、放送送信制御部２１３から共通制御情報制御部２１２へ共通制御パケットの作成命令がなされる。この命令によって共通制御情報制御部２２１は、共通制御情報作成部２０９にチャネルキーＤＢ２１１を検索して、最小のチャネルキーＩＤを持つチャネルキーデータを検索するように指示する。共通制御情報作成部２０９はこれを受けてチャネルキーＤＢ２１１を検索してチャネルキーデータを取得する（ステップＳ４０１）。

【０１３５】また、放送送信制御部２１３から個別制御情報制御部２０６へ個別制御パケットの作成命令がなされる。この命令によって個別制御情報制御部２０６は個別制御情報作成部２０３に加入者ＤＢ２０２を検索して、放送送信フラグが「１」である最小の加入者ＩＤを持つ加入者データを検索するように指示する。個別制御情報作成部２０６はこれを受けて加入者ＤＢ２０２を検索して加入者データを取得する（ステップＳ４０６）。

【０１３６】一方、共通制御情報作成部２０９では、取得したチャネルキーデータからチャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）を取得し、図8に示したような共通制御パケットを作成する（ステップＳ４０４）。その際、チャネル識別子をキーにしてワーク鍵ＤＢ２１０を検索し、当該チャネルに対する有効なワーク鍵を抽出し、当該ワーク鍵を使って共通制御パケットの暗号化されるべき部分を暗号化する。更に、当該ワーク鍵のワーク鍵識別子と情報識別子を付けて共通制御パケットを生成し、共通制御情報制御部２１２、放送送信制御部２１３を経由して放送送信部２１４へ送り、放送送信部２１４では当該パケットを放送波に載せて発信する（ステップＳ４０５）。

【０１３７】次に、個別制御情報作成部２０６では、取得した加入者データからチャネル契約情報を抽出し、これに基づいて必要なワーク鍵をワーク鍵ＤＢ２０４から取得する（ステップＳ４０７）。双方向通信により配信する場合と同様、ワーク鍵と当該加入者データ中の受信装置ＩＤ、チャネル契約情報からデジタル署名以外の契約情報本体を作成し、デジタル署名生成鍵格納部２０５に格納されているデジタル署名生成鍵を用いて契約情報を作成する。更に当該加入者データ中のマスター鍵で契約情報を暗号化し、マスター鍵識別子や情報識別子を付加して個別制御パケットを作成する（ステップＳ４０８）。作成したパケットは個別制御情報制御部２０６を経由して、放送送信制御部２１３に渡され、ここから当該パケットを放送波に載せて発信する（ステップＳ４０９）。

【０１３８】上記処理動作は、共通制御パケット（チャネルキー配信用の共通制御パケット）と個別制御パケット（契約情報配信用の個別制御パケット）を交互に放送送信する例を示している。しかし、この前者をどのくらい配信したら後者をどのくらい配信するかといった配信割合は本来放送事業者の都合に合わせて決められるものであり、割合の変更は容易に実現可能である。

【０１３９】図３６の説明に戻り、１組の共通制御パケットと個別制御パケットの送信が終了した段階で、それぞれ次の送信パケットの生成に入る。即ち、共通制御情報制御部２１２においては放送送信制御２１３からの指示により次のチャネルキーデータをチャネルキーＤＢ２１１から抽出する（ステップＳ４１０）。ここで次のチャネルキーデータとは、先に送信した共通制御パケットに係るチャネルキーデータのチャネルＩＤの次に大きいチャネルＩＤを持つチャネルキーデータである。ここでそのようなチャネルキーデータがなかった場合は、最小のチャネルＩＤを持つチャネルキーデータをチャネルキーＤＢ２１１から抽出する（ステップＳ４１４）。

【０１４０】また、加入者データに関しても同様に、放送送信フラグが「１」である加入者データのうち加入者ＩＤが前記処理済みの加入者データの加入者ＩＤを越えた中で最小のものを抽出する（ステップＳ４１２）。ここで、そのような加入者データがなければ、最小の加入者ＩＤを持つ加入者データを抽出する（ステップＳ４０２）。

【０１４１】これら抽出したデータはそれぞれ共通制御情報作成部２１２、個別制御情報作成部２０３において前述したようなパケット作成／送信処理を行う。このようにして放送開始から間断なく動き続ける。

【０１４２】以上の説明からも明らかなように、共通制御パケットの生成と個別制御パケットの生成は並列に行うことができる。これは２種類のパケットの生成／送信を放送送信制御部２１３で制御して一定の割合で送信することができるからである。

【０１４３】（第６の実施形態）次に、いくつかのバリエーションを述べる。第１のバリエーションとして、センターから電源オンコマンドを各受信装置に個別に配信

するという第２の実施形態に係る放送受信装置に対しコマンドパケット、個別制御パケット、共通制御パケットを配信するためのセンター側に設けられた情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。この第１のバリエーションは第６の実施形態として説明する。

【０１４４】第２のバリエーションとして、センターから発呼コマンドを各受信装置に個別に配信して、受信装置側からセンターに発呼させるという第３の実施形態に係る放送受信装置に対し、コマンドパケット、個別制御パケット、共通制御パケットを配信するためのセンター側に設けられた情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。この第２のバリエーションは第７の実施形態として後述する。

【０１４５】第６の実施形態に係る情報配信装置の要部の構成例は、第５の実施形態の場合（図３２）と同様であるが、処理動作が異なる。まず、放送波にて電源オンコマンドパケットを配信してから双方向通信により個別制御情報を配信する場合について、図３７～図３８に示すフローチャートに沿って説明する。

【０１４６】この処理は、契約変更時期（例えば１ヶ月毎）に合わせて開始される。個別制御情報制御部２０６は、契約変更時期が来たら、まず個別制御情報作成部２０６へチャネル契約情報等の更新をするための契約情報を送信すべき受信装置であって、まだ、その契約情報を送信していない受信装置に対し順次電源オンコマンドを送信する旨の命令を行う。個別制御情報作成部２０３はこれを受け、加入者ＤＢ２０２を検索して、送信済みフラグが「０」の加入者データを加入者ＩＤが小さいものから最大M個取り出す（ステップＳ５０１）。ここで、Mは電源オンコマンドパケットの情報容量その他で決まる定数である。

【０１４７】次に抽出された加入者データからそれぞれ受信装置ＩＤを抽出し（ステップＳ５０２）、抽出された受信装置ＩＤとそれら受信装置ＩＤの数の並びに対しデジタル署名を付すため、デジタル署名生成鍵格納部２０５からデジタル署名生成鍵を抽出して（ステップＳ５０４）、当該鍵で受信装置ＩＤとそれら受信装置ＩＤの数を暗号化してデジタル署名を生成する（ステップＳ５０５）。抽出された受信装置ＩＤとそれら受信装置ＩＤの数とデジタル署名と電源オンコマンドのコマンド識別子とから図１７に示すようなデータ形式のコマンド本体を作成する。このようにしてできたコマンド本体に情報識別子を付け、コマンドパケットが生成される（ステップＳ５０６）。生成されたコマンドパケットは個別制御情報制御部２０６を経由して放送送信部２１４に送られて（ステップＳ５０７）、一時、放送送信部２１４内のバッファメモリに格納され、後述する手順で共通制御パケットと共に放送送信される（図３９参照）。

【０１４８】次に、チャネル契約情報等を更新しなければならない放送受信装置に、そのための個別制御パケットを配信する処理を行う。ｉ＝１として（ステップＳ５０８）、ステップＳ５０１で抽出された（最大）M個の加入者データのうち、ｉ番目の加入者データ中のチャネル契約情報に基づいてワーク鍵ＤＢ２１０からワーク鍵を抽出する（ステップＳ５０９）。更に第５の実施形態の説明と同様にして、個別制御パケット（契約情報配信用の個別制御パケット）を作成する（ステップＳ５１０）。次に当該加入者データ内にある発呼番号を用いて発呼し（ステップＳ５１１）、発呼先の放送受信装置と双方向通信を開始する。ここで当該受信装置から応答がない場合は（ステップＳ５１２）、受信エラーの旨のエラーを個別制御情報制御２０６に返し、個別制御信情報制御部２０６ではこれをエラー出力部２１５で表示させ（ステップＳ５２２）、図３８のステップＳ５１６へ進み、次の加入者データへ処理を移す。

【０１４９】ステップＳ５１２で、発呼先の放送受信装置から応答が返ってきた場合は、作成した個別制御パケットを送信する（ステップＳ５１３）。個別制御パケット送信後、予め定められた所定時間を経過するまでに、当該受信装置から受領通知がなかった場合は（ステップＳ５１４）、受領エラーの旨のエラーを個別制御情報制御部２０６に返し、個別制御情報制御部２０６では、エラー出力部２１５に受領エラーの旨を表示させ、図３８のステップＳ５１６へ進み、次の加入者データへ処理を移す。

【０１５０】ステップＳ５１４で受領通知があった場合は、図３８のステップＳ５１５へ進み、当該ｉ番目の加入者データの送信済みフラグを「１」にして、ステップＳ５１６へ進み、次の加入者データに処理を移す。

【０１５１】次の加入者データに処理を移す際、以下の処理が必要である。即ち、ｉ＝ｉ＋１として（ステップＳ５１６）、ｉがMを越えないか否かをチェックする（ステップＳ５１７）。越えない場合はｉ番目の加入者データが存在すれば（ステップＳ５１８）、ステップＳ５０９へ戻り、以降、前述同様、その加入者データに対して処理を行う。ステップＳ５１８で、加入者データが存在しない場合は、ステップＳ５１９へ進み、加入者ＤＢ２０２を検索して送信済みフラグが「０」の次の（最大）M個のレコードを抽出する（ステップＳ５１９）。ここで１個以上の加入者データが抽出できれば（ステップＳ５２０）、ステップＳ５０２へ戻り、その加入者データ群に対しての電源オンコマンドの作成を行う。ステップＳ５２０で、加入者ＤＢ２０２から１つも加入者データが抽出されなかった場合は、一回り処理が終了したことになるので、加入者ＤＢ２０２の全ての加入者データを検索して送信済みフラグが「０」のものがあるか否かを確認する（ステップＳ５２１）。ここであれば、ステップＳ５０１へ戻り、以降、前述同様である。ステッ

プＳ５２１で送信済みフラグが「０」のものが無ければ全ての加入者データに関して送信済みなので終了する。

【０１５２】一方、ステップＳ５１７で、ｉがＭを越えた場合は、電源オンコマンドを放送送信した受信装置への個別制御パケットは送信し終えたことになるので、ステップＳ５１９へ進み、加入者ＤＢ２０２を検索して、送信済みフラグが「０」である次の（最大）Ｍ個の加入者データを抽出する。ここで１個以上の加入者データが抽出できれば（ステップＳ５２０）、その加入者データ群に対して電源オンコマンドを作成するところ（ステップＳ５０２）に戻って繰り返す。ステップＳ５２０で１つも加入者データが抽出されなかった場合は一回り処理が終了したことになるので、加入者ＤＢ２０２の全ての加入者データを検索して送信済みフラグが「０」のものがあるか否かを確認する（ステップＳ５２１）。ここで１つでも加入者データが抽出されれば、ステップＳ５０１の処理の最初に戻る。１つも加入者データが抽出されなければ、全ての加入者データに関して送信済みなので終了する。

【０１５３】以上が電源オンコマンドを放送配信した後、個別制御パケットを双方向通信にて送信するまでの処理動作である。本実施形態によれば、これから個別制御パケットを双方向通信にて送信する図１に示したような構成の放送受信装置に対して、予め放送波経由で双方向通信に係る構成部の電源をオンにする指示を出し、当該放受信装置を着信待ち状態にした後、センター側（図３２の情報配信装置）から個別制御パケット配信のための発呼を行うので、双方向通信にて個別制御パケットを受信可能な放送受信装置に対しては、確実に個別制御パケットを双方向通信にて配信することができる。

【０１５４】次に、共通制御パケットの送信情報の送信処理動作について、図３９に示すフローチャートに沿って説明する。この処理は、放送開始時に開始され、以降放送終了まで間断なく続けられる。

【０１５５】まず、共通制御情報制御部２１２から共通制御情報作成部２０９に対して、最小のチャネルキーＩＤを持つチャネルキーデータを検索するように指示する（ステップＳ６０１）。共通制御情報作成部２０９ではこの指示を受けてチャネルキーＤＢ２１１を検索し、チャネルキーを取得する。更に、取得したチャネルキーデータからチャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）を取得し、図８に示したような共通制御パケットを作成する（ステップＳ６０２）。その際、チャネル識別子をキーにしてワーク鍵ＤＢ２１０を検索し、当該チャネルに対する有効なワーク鍵を抽出し、当該ワーク鍵を使って共通制御パケットの暗号化されるべき部分を暗号化する。更に、当該ワーク鍵のワーク鍵識別子と情報識別子を付けて共通制御パケットを生成し、共通制御情報制御部２１２、放送送信制御部２１３を経由して放送送信部２１４へ送り、放送送信部２１４では当該パケットを放送波に載せて発信する（ステップＳ６０３）。

【０１５６】次に、放送送信部２１４は、図３７のステップＳ５０１～ステップＳ５０７の処理で作成された電源オンコマンドパケットがそのバッファメモリ内に存在するか否かチェックして（ステップＳ６０４）、存在する場合は当該コマンドパケットの内、作成された時が最も古いものを放送送信部２１４から放送送信し（ステップＳ６０５）、ステップＳ６０６へ進み、一方、存在しない場合は、ステップＳ６０５をスキップして、ステップＳ６０６へ進む。

【０１５７】ステップＳ６０６では、次のチャネルキーＩＤのチャネルキーデータをチャネルキーＤＢ２１１から検索する旨の命令が放送送信制御部２１３から共通制御情報制御部２１２を経由して共通制御情報作成部２０９に伝えられ、共通制御情報作成部２０９ではチャネルキーＤＢ２１１を検索してチャネルキーデータの抽出を行なう（ステップＳ６０６）。ここで、抽出に成功した場合は（ステップＳ６０７）、ステップＳ６０２以降の当該チャネルキー配信用の共通制御パケットの作成／送信処理を行ない、抽出に失敗してしまった場合は、ステップＳ６０１の処理最初に戻り、再び最小のチャネルキーＩＤをもつチャネルキーデータを検索する。

【０１５８】このように、１または複数の電源オンコマンドパケット（より一般的に言えばコマンドパケット）をチャネルキー配信用の共通制御パケットを１または複数個配信する際に送信することにより、チャネルキー配信用の共通制御パケットの送信にも支障をきたさず、タイムリーにコマンドパケットを送信することができる。

【０１５９】尚、通常（タイムリーな受信開始のため）チャネルキーは１秒間に２回は送信しなくてはならないのに対して、電源オンコマンドの発行頻度は個別制御パケットの送信時間などから１秒に１回もないと考えられる。このため、共通制御パケット配信時に占める配信すべき電源オンコマンドパケット数の割合は極めて低い。更に、このことから電源オンコマンドパケットが作成され、それが放送送信制御部２１３に送られた後すぐに送信されることが期待できるため、個別制御パケット送信のため放送受信装置を発呼する際には、既に受信装置側の双方向通信回線の電源がオンになっていると考えて良い。

【０１６０】（第７の実施形態）センターから発呼コマンドを各受信装置に個別に配信して、受信装置側からセンターに発呼させるという第３の実施形態に係る放送受信装置に対し、コマンドパケット、個別制御パケット、共通制御パケットを配信するためのセンター側に設けられた情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。

【０１６１】第７の実施形態に係る情報配信装置の要部

の構成例を図４０に示し、コマンドパケットの作成処理動作について、図４０を参照しながら図４１に示すフローチャートに沿って説明する。この処理動作は、チャネル契約情報等の変更時期に合わせて、例えば１ヶ月毎に開始される。個別制御情報制御部２０６はチャネル契約情報等の変更時期が来たら、まず個別制御情報作成部２０３へチャネル契約情報未更新の受信装置に対し順次発呼コマンドを送信する旨の命令を行う。個別制御情報作成部で２０３は、これを受け、加入者ＤＢ２０４を検索して、送信済みフラグが「０」の加入者データを加入者ＩＤが小さいものから最大M個取り出す（ステップＳ６１１）。抽出された受信装置ＩＤとそれら受信装置ＩＤの数の並びに対しデジタル署名を付すため、デジタル署名生成鍵格納部２０５からデジタル署名生成鍵を抽出して（ステップＳ６１２）、当該鍵で受信装置ＩＤとそれら受信装置ＩＤの数、あるいはそれらデータ列とその特徴量としてのハッシュ値を暗号化してデジタル署名を生成する（ステップＳ６１３）。抽出された受信装置ＩＤとそれら受信装置ＩＤの数とデジタル署名と発呼コマンドのコマンド識別子とから図１７に示すようなデータ形式のコマンド本体を作成する。このようにしてできたコマンド本体に情報識別子を付け、発呼コマンドパケットが生成される（ステップＳ６１４）。

【０１６２】生成された発呼コマンドパケットは、個別制御情報制御部２０６を経由して個放送送信制御部２１３に送られて（ステップＳ６１５）、以下に示すように、他の共通制御パケットとともに放送送信される。

【０１６３】双方向通信による個別制御パケットの送信処理動作について、図４０を参照しながら、図４２～図４３に示すフローチャートに従って説明する。この処理は、放送受信装置からの発呼によって開始される（ステップＳ７０１）。センターでは受信装置から発呼をモデム２０８を経由して送受信制御部２０７で受け（ステップＳ７０２）、送受信制御部２０７では、チャレンジ作成部２５２に対し、受信装置ＩＤを尋ねるチャレンジの作成命令を送る。チャレンジ作成部２５２ではこれを受けて受信装置ＩＤを尋ねる図２３に示した構成のチャレンジパケットを作成する。ここでチャレンジデータベース（ＤＢ）２５１とは、各種チャレンジのチャレンジ番号と処理の組が記載されたデータベースである。チャレンジ作成部２５２は、チャレンジＤＢ２５１から受信装置ＩＤを問い合わせるチャレンジ番号をキーにして処理内容を抽出する。作成されたチャレンジパケットは送受信部２０７からモデム２０８を経由して受信装置に送信される（ステップＳ７０３）。送信後予め定められてた所定時間内に当該受信装置からレスポンスパケットが送信されてこなかった場合（ステップＳ７０４）、個別制御情報制御部２０６は、受信装置ＩＤを尋ねるチャレンジ失敗の旨のエラー出力をエラー出力部２１５から出力して当該受信装置に対する処理を終了する（ステップＳ７１７）。

【０１６４】ステップＳ７０４で所定時間内にレスポンスパケットが送信されてきた場合は、そのレスポンスパケットは送受信制御部２０７からレスポンス検証部２５３に送られる。レスポンス検証部２５３では、当該レスポンスパケットのフォーマット検査を行なった後、そのパケットから取り出した受信装置ＩＤを送受信制御部２０７に出力する（ステップＳ７０５）。送受信制御部２０７は、この受信装置ＩＤをキーに個別制御情報制御部２０６に対し、加入者ＤＢ２０２から当該受信装置ＩＤの加入者データを抽出する旨命令する。ここで、該当する加入者データがなければ当該受信装置ＩＤは存在しないので（ステップＳ７０５）、エラー出力等を行って処理を終了する（ステップＳ７２２）。加入者データを取得したら（ステップＳ７０６）、当該加入者データを送受信制御部２０７へ送り、送受信制御部２０７はレスポンス検査部２５３へそれを送る。

【０１６５】その後、送受信制御部２０７がチャレンジ作成部２５２に対し、受信装置ＩＤを尋ねるチャレンジ作成の場合と同様、マスター鍵識別子を尋ねるチャレンジ作成を指示し、その結果作成されたチャレンジパケットが送信され（ステップＳ７０７）、所定時間内に送られてきたレスポンスパケットを検査する（ステップＳ７０８、ステップＳ７０９）。マスター鍵識別子が当該加入者データのそれと一致していなかった場合は、マスター鍵識別子不一致の旨のエラー出力を行い（ステップＳ７１９）、一致していた場合は以下に説明する受信装置認証の処理に移る。

【０１６６】受信装置認証処理は、正当な受信装置でしか知らない情報を使って答えさせるチャレンジを１つ以上発生させ、そのレスポンスで認証を行う処理である。まず送受信制御部２０７では、ｊ＝１に設定し（ステップＳ７１０）、チャレンジ作成部２５２に対して認証チャレンジを発行するように要請する。要請を受けたチャレンジ作成部２５２ではチャレンジＤＢ２５１からランダムにチャレンジを抽出し、図２３に示すようなチャレンジパケットを作成し（ステップＳ７１１）、送受信制御部２０７からモデム２０８を介して放送受信装置へ送信される（ステップＳ７１２）。送信後一定期間内に受信装置からレスポンスパケットが送られてこなかった場合（ステップＳ７１３）、認証チャレンジ失敗の旨のエラー出力を行い、終了する（ステップＳ７２０）。レスポンスパケットが送られてきた場合、そのレスポンスパケットは送受信制御部２０７からレスポンス検証部２５３に送られ、レスポンス検証部２５３においてチャレンジＤＢ２５１に定められた認証アルゴリズムによって認証検査を行う（ステップＳ７１４）。認証検査が成功した場合は正しいレスポンスであることが示されたので、ｊを１つインクリメントして（ステップＳ７１５）、ｊがNを越えるか否かチェックする（ステップＳ７１

６）。Nは予めシステムに依存した定数で、認証チャレンジの試行回数を意味する。ｊがNを越えない場合、ｊがNを越えるまでステップＳ７１１～ステップＳ７１４の受信装置認証処理を繰り返す。また、ステップＳ７１４で認証検査が失敗した場合は、間違ったレスポンスであるので認証失敗の旨のエラー出力を行い終了する（ステップＳ７２１）。

【０１６７】ステップＳ７１６でｊがNを越えた場合は、認証が終了したことを意味し、情報配信装置（センター）側で現在通信を行っている受信装置が正当なものであることを確認できたことになる。そこで、図４３のステップＳ７２２へ進み、送受信制御部２０７から認証終了の信号を個別制御情報制御部２０６に送り、個別制御情報制御部２０６は当該加入者データの個別制御パケットを作成するよう、個別制御情報作成部２０３に要請する。個別制御情報作成部２０３ではこれを受けて、当該加入者データ中のチャネル契約情報に基づいて必要なワーク鍵をワーク鍵ＤＢ２１０から取得する（ステップＳ７２２）。ここでは、ワーク鍵はチャネル毎に設定されていると仮定しているので、チャネル契約情報にて指定される契約しているチャネル分だけのワーク鍵を取得する処理が必要になる。

【０１６８】次に、取得されたワーク鍵とワーク鍵識別子のペア及び当該加入者データの受信装置ＩＤ、チャネル契約情報からデジタル署名以外の契約情報本体を作成し、デジタル署名生成鍵を用いて契約情報を作成する。更に当該加入者データのマスター鍵で契約情報を暗号化し、マスター鍵識別子や情報識別子を付加して、図２２に示したような個別制御パケットを作成する（ステップＳ７２３）。作成したパケットは個別制御情報制御部２０６を経由して送受信制御部２０７へ送られ、受信装置へ送信される。当該送信後、一定期間に受信装置より受領通知があった場合は（ステップＳ７２４）当該加入者データの送信済みフラグを「１」にして終了する（ステップＳ７２５）。受領通知がなかった場合は個別制御パケットの受領失敗の旨のエラー出力を行い終了する（ステップＳ７２６）。

【０１６９】上記第７の実施形態によれば、一時期に受信装置側からの発呼が集中しないように、受信装置側からの発呼の時期をセンター側から調整でき、更に受信装置側からの発呼であっても受信装置の正当性を認証した後、受信装置に格納されているチャネル契約情報等を更新するための個別制御パケットの送信が行えるため、他の受信装置になりすまして発呼するような不正を防止できる。

【０１７０】以上の説明からも明らかなように第１のバリエーションはセンター発呼を前提にし、第２のバリエーションは受信装置発呼を前提にしているため、同時にこれを行なうことも可能である。即ち、発呼コマンドパケットを送信しても一向に発呼してこない受信装置に関して電源オンコマンドパケットを送信してセンター発呼したり、それでも受信しない場合は放送波で個別制御パケットを送信するように構成するのである。このようにすると、より個別制御パケットの送信機会が増え、不正視聴が防げるばかりか、契約しているのに契約更新されないようなトラブルも減る。

【０１７１】更に、これらと第５の実施形態を組み合わせて、例えば、センター発呼による双方向通信による個別制御パケットの送信を基本にするが、応答しない受信装置については、電源オンコマンドパケットを放送配信して強制的に受信装置の有する双方向通信機能部を着呼可能な状態（電源オン状態）にしたり、発呼コマンドパケットを放送送信して受信装置側から発呼させるなどして、複数の方法により受信装置に記憶されているチャネル契約情報等の更新のための個別制御パケットを配信することができる限定受信システムが構築できる。特にモバイル環境の携帯可能な受信装置に関しては（受信装置が常に同じ状態ではないので）個別制御パケットの送信手段をより多く持っていることは有利である。

【０１７２】（第８の実施形態）第８の実施形態は第４の実施形態で説明した放送受信装置に対し、個別制御情報、共通制御情報を配信するためのセンター側に設けられた情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。

【０１７３】第８実施形態は第５～第７の実施形態と情報配信装置と構成、処理動作の上で重複する部分が多いので異なる部分のみを説明するに留める。すなわち、個別制御パケットはデータ構成に若干の違いはあってもその取り扱いは同じであり、そのため個別制御パケットを双方向通信にて配信するための構成部と処理動作は第５～第７の実施形態の場合と同様である。そこで、以下では、個別制御パケット共通制御パケットを放送配信する構成部とその処理動作に絞って説明する。

【０１７４】第５～第７の実施形態では放送送信部２１４から送信されるのは、チャネルキー配信用の共通制御パケットとチャネル契約情報等の配信用の個別制御パケットであったのに対し、第８の実施形態ではチャネルキー配信用の共通制御パケットと、マスター鍵生成情報配信用の共通制御パケットと、チャネル契約情報配信用の個別制御パケットの３つが仮定される。従って。第８の実施形態では上記３種類のパケットを放送送信しなくてはならない。この点が第５～第７の実施形態と本質的に異なる点である。

【０１７５】第８の実施形態に係る情報配信装置の要部の構成例を図４４に示し、図４５～図４６に上記３種類のパケットを放送送信する際の処理動作を示している。以下、図４４を参照しながら、図４５～図４６に示すフローチャートに沿って説明する。

【０１７６】この処理は、放送開始と同時に開始され、放送が続く間間断なく繰り返される。まず、共通制御情

報作成部２０９はチャネルキーＤＢ２１１を検索して、最小のチャネルＩＤを持つチャネルキーデータを取得する。ここでチャネルキーデータはチャネルキーＤＢ２１１に登録されているチャネル毎の少なくともチャネルキーを含むデータで図３４に示す構造をしている。チャネルキーデータは、チャネルＩＤとチャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）からなっている。ここでチャネルＩＤとは各チャネルにふられるデータベース管理上の番号である。チャネル識別子は受信装置が各チャネルを識別するための情報で前述した実施形態の説明と同様である。更にチャネルキー識別子及びチャネルキーも前述した実施形態の説明と同様である。ここでチャネルキーとその識別子のペアが２組存在するのは現在有効なチャネルキーと次に使われるチャネルキーを一緒に送信する必要があるためであり、構成によっては現在使用されているチャネルキーのみでも構わない。

【０１７７】まず、放送送信制御２１３から共通制御情報制御部２１２へチャネルキー配信用の共通制御パケットの作成命令がなされる。この命令によって共通制御情報制御部２１２は共通制御情報作成部２０９にチャネルキーＤＢ２１１を検索して、最小のチャネルＩＤを持つチャネルキーデータを検索するように指示する。共通制御情報作成部２０９はこれを受けてチャネルキーＤＢ２１１を検索して、チャネルキーデータを取得する（ステップＳ８０１）。

【０１７８】また、放送送信制御部２１３は、個別制御情報制御部２０６へ個別制御パケットの作成命令を出す。この命令によって個別制御情報制御部２０６は個別制御情報作成部２０３に加入者ＤＢ２０２を検索して、放送送信フラグが「１」である最小の加入者ＩＤを持つ加入者データを検索ように指示する。個別制御情報作成部２０３は、これを受けて加入者ＤＢ２０２を検索して、加入者データを取得する（ステップＳ８０２）。

【０１７９】次に、共通制御情報作成部２０９では、取得したチャネルキーデータからチャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）を取得し（ステップＳ８０３）、図３０（ｂ）に示したようなチャネルキー配信用の共通制御パケットの作成を開始する。すなわち、マスター鍵格納部２６１から有効なマスター鍵を抽出し、当該マスター鍵を使って、チャネル識別子、チャネルキー識別子（１）、チャネルキー（１）、チャネルキー識別子（２）、チャネルキー（２）からなるデータ列を暗号化する。更に、当該マスター鍵のマスター鍵識別子と情報識別子を付けてチャネルキー配信用の共通制御パケットを生成する（ステップＳ８０４）。この共通制御パケットは、共通制御情報制御部２１２、放送送信制御部２１３を経由して放送送信部２１４へ送られ、ここから放送波に載せて発信される（ステップＳ８０５）。

【０１８０】次に、個別制御情報作成部２０３では、取得した加入者データから受信装置ＩＤ、チャネル契約情報を取得し（ステップＳ８０６）、それらからデジタル署名以外の契約情報を作成する。更にデジタル署名生成鍵格納部２０５に格納されているデジタル署名生成鍵を用いて受信装置ＩＤからチャネル契約情報までのデータ列、あるいは、このデータ列とその特徴量としてのハッシュ値とを暗号化してデジタル署名を作成して、それを受信装置ＩＤからチャネル契約情報までのデータ列の最後に付して、図２９に示したような契約情報を作成する。更に当該加入者データから取り出したマスター鍵で契約情報を暗号化し、マスター鍵識別子、受信装置ＩＤ、情報識別子を付加して、図７（ｂ）に示したような個別制御パケットを作成する（ステップＳ８０７，ステップＳ８０８）。

【０１８１】作成したパケットは個別制御情報制御部２０６、放送送信制御部２１３を経由して放送送信部２１４へ送られ、ここから放送波に載せて発信される（ステップＳ８０９）。

【０１８２】次に、共通制御情報作成部２０９は、マスター鍵生成情報配信用の共通制御パケットの作成を行う。まず、マスター鍵生成情報格納部２６４からマスター鍵生成情報とそれから生成されるマスター鍵の識別子（マスター鍵識別子）を取得し、続いて、デジタル署名生成鍵格納部２０５からデジタル署名生成鍵を取得してマスター鍵生成情報あるいはマスター鍵生成情報とその特徴量としてのハッシュ値とを暗号化することによりマスター鍵生成情報に対するデジタル署名を作成し、デジタル署名と情報識別子を付加して、図３０（ａ）に示す構成のマスター鍵生成情報配信用の共通制御パケットを作成する（ステップＳ８１０～ステップＳ８１１）。

【０１８３】この作成されたパケットは、共通制御情報制御部２１２、放送送信制御部２１３を経由して放送送信部２１４へ送られ、ここから放送波に載せて発信される（ステップＳ８１２）。

【０１８４】なお、以上の説明では、チャネルキー配信用の共通制御パケット、契約情報配信用の個別制御パケット、マスター鍵生成情報配信用の共通制御パケットを順次放送送信する例を示している。しかし、どのパケットをどれだけ送信したら次のパケットをどれだけ送信するかといったパケットの送信量にの割合は、本来放送事業者の都合に合わせて決められるものであり、割合の変更は容易である。

【０１８５】チャネルキー配信用の共通制御パケット、契約情報配信用の個別制御パケット、マスター鍵生成情報配信用の共通制御パケットの１組の送信が終了した段階で、次に送信すべきパケットの生成に移る。即ち、共通制御情報作成部２０９は、次のチャネルキーデータをチャネルキーＤＢ２１１から検索する（ステップＳ８１

３）。ここで次のチャネルキーデータとは先に送信したパケットに係るチャネルキーデータのチャネルＩＤより大きいチャネルＩＤを持つチャネルキーデータのうちチャネルＩＤが最小のものである。ここでそのようなチャネルキーデータがなかった場合は（ステップＳ８１４）、最小のチャネルＩＤを持つチャネルキーデータをチャネルキーＤＢ２１１から抽出する（ステップＳ８１７）。

【０１８６】また、加入者データに関しても同様に、放送送信フラグが「１」である加入者データのうち加入者ＩＤが前記処理済みの加入者データの加入者ＩＤの値より大きいもののうち、最小のものを抽出する（ステップＳ８１５）。ここで、そのような加入者データがなければ（ステップＳ８１６）、最小の加入者ＩＤを持つ加入者データを抽出する（ステップＳ８０２）。

【０１８７】このようにして抽出されたチャネルキーデータ、加入者データを基に、前述の説明従って、チャネルキー配信用の共通制御パケットと契約情報配信用の個別制御パケットの作成／送信処理を行ない、その後、マスター鍵生成情報配信要の共通制御パケットの作成／送信処理を行なう。以上の処理を放送開始から間断なく動き続ける。

【０１８８】なお、チャネルキー配信用の共通制御パケットと契約情報配信用の個別制御パケットとマスター鍵生成情報配信用の共通制御パケットの生成は並列に行うことができる。そのように実装する際には３種類のパケットをそれぞれどれくらいづつ作成してどれくらいづつ送信するかといった生成／送信制御を放送送信制御部２１３で行い一定の割合で生成／送信すればよい。

【０１８９】また、容易に分かるように、第５～第７の実施形態は第８の実施形態と組み合わせて用いることも可能である。

【０１９０】（追記）尚、チャネル数が少ない放送においては、チャネル契約情報を用いずに、ワーク鍵のみによる限定受信も可能である。実際、ワーク鍵は、チャネル毎に設定されている鍵なので、このワーク鍵を契約期間（例えば１ヶ月）毎に更新し、更新されたワーク鍵を当該契約期間に当該チャネルを視聴している視聴者のみに個別制御情報として送信することにより、契約者のみへの視聴限定ができる。

【０１９１】このような構成において、受信装置側は、当該チャネルのチャネルキーが共通制御パケットで送信されてきたとき、共通制御パケットのヘッダ部分に記載されているワーク鍵識別子をキーにして、当該チャネルのワーク鍵がワーク鍵格納部に存在するかをチェックする。存在した場合には当該制御パケットの暗号化部を復号し、当該チャネルのチャネルキーを取得する。存在しなかった場合は当該共通制御パケットに対する処理を終了する。このことから当該チャネルのワーク鍵を持っている当該チャネルの視聴契約者だけが当該チャネルキーを取得できるため、限定受信が実現できる。

【０１９２】このように、各チャネルのワーク鍵を契約期間毎に更新するだけでも、限定受信システムは構成できる。ただし、現在のＣＳ放送のようにチャネル数が多い場合、ワーク鍵を契約期間毎に変更するとワーク鍵の更新情報が大規模になるため現実的でない。それ故に現在のＣＳ放送においては上記第１～第８の実施形態で説明したようなチャンネル契約情報を併用する方式が望ましい。しかし、例えば、１チャネルしかない（もしくは、契約形態が１つしかない）放送においては、ワーク鍵は１つで充分なので、上記のようなワーク鍵のみによる限定受信システムもメリットがある。

【０１９３】なお、第１の実施形態およびそれに関連する実施形態において、受信装置にて記憶されるチャネル契約情報、ワーク鍵は、１つの個別制御パケットにて同時に更新してもよいし、どちらか一方のみを更新するようにしてもよい。

【０１９４】また、第１～第８の実施形態において、デジタル署名を作成する際、デジタル署名の対象である情報部分とその特徴量としてのハッシュ値とを暗号化してデジタル署名を作成してもよい。すなわち、例えば、図５の契約情報中のデジタル署名であれば、デジタル署名以外の部分とそのハッシュ値とを暗号化して契約情報のデジタル署名を作成してもよい。

【０１９５】なお、本発明は、上記第１～第８の実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。さらに、上記実施形態には種々の段階の発明は含まれており、開示される複数の構成用件における適宜な組み合わせにより、種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題（の少なくとも１つ）が解決でき、発明の効果の欄で述べられている効果（少なくとも１つ）が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【０１９６】

【発明の効果】以上説明したように、本発明によれば、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る放送受信装置の要部の構成例を示した図。

【図２】チャネル契約情報の一例を示した図。

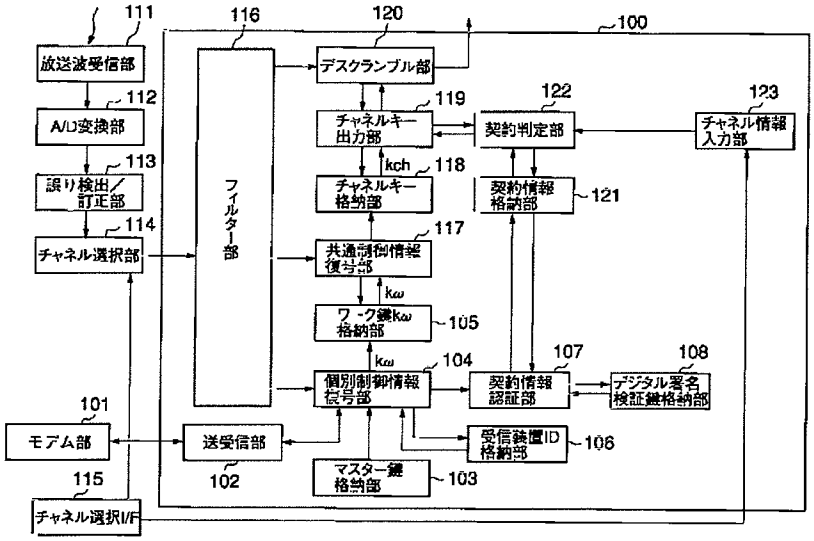
【図３】限定受信システムで用いられる鍵構成の一例を示した図。

【図４】コンテンツパケットのデータ構成の一例を示した図。

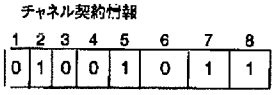
【図５】契約情報の一例を示した図。
【図６】チャネル契約情報の他の例を示した図。
【図７】個別制御パケットのデータ構成の一例を示した図。
【図８】共通制御パケットのデータ構成の一例を示した図。
【図９】図１に示した放送受信装置の双方向通信による個別制御パケット受信処理動作を説明するためのフローチャート。
【図１０】図１に示した放送受信装置の放送波による個別制御パケット／共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。
【図１１】放送波による個別制御パケット／共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。
【図１２】チャネル選択／チャネルキー取得処理動作を説明するためのフローチャート。
【図１３】放送波による個別制御パケット／共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。
【図１４】放送波による個別制御パケット／共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。
【図１５】本発明の第２の実施形態に係る放送受信装置の要部の構成例を示した図。
【図１６】コマンドパケットのデータ構成例を示した図。
【図１７】コマンド本体のデータ構成例を示した図。
【図１８】図１５の放送受信装置の放送波による個別制御パケットの受信処理動作を説明するためのフローチャート。
【図１９】本発明の第３の実施形態に係る放送受信装置の要部の構成例を示した図。
【図２０】図１９の放送受信装置の放送波による個別制御パケットの受信処理動作を説明するためのフローチャート。
【図２１】双方向通信で送受信されるパケットのデータ構成例を示した図。
【図２２】個別制御パケットのデータ構成例を示した図。
【図２３】チャレンジパケットのデータ構成例を示した図。
【図２４】レスポンスパケットのデータ構成例を示した図。
【図２５】受信装置が発呼コマンドを受けた後の処理動作を示したフローチャート。
【図２６】受信装置が発呼コマンドを受けた後の処理動作を示したフローチャート。
【図２７】本発明の第４の実施形態に係る放送受信装置の要部の構成例を示した図。
【図２８】第４の実施形態に係る限定受信システムで用いられる鍵構成の一例を示した図。
【図２９】第４の実施形態に係る契約情報の一例を示した図。
【図３０】共通制御パケットのデータ構成例を示した図で、（ａ）図はマスター鍵生成情報配信用の共通制御パケットの場合、（ｂ）図はチャネルキー配信用の共通制御パケットの場合を示している。
【図３１】共通制御パケットの受信処理動作を説明するためのフローチャート。
【図３２】本発明の第５の実施形態に係る個別制御情報の情報配信装置であって、第１の実施形態に係る放送受信装置（図１）に対応する情報配信装置の要部の構成例を示した図。
【図３３】図３２の加入者データベースに格納されている加入者データの一例を示した図。
【図３４】図３２のチャネルキーデータベースに格納されているチャネルキーデータの一例を示した図。
【図３５】図３２の情報配信装置の処理動作を説明するためのフローチャート。
【図３６】図３２の情報配信装置の処理動作を説明するためのフローチャート。
【図３７】本発明の第６の実施形態に係る情報配信装置の放送波にて電源オンコマンドパケットを配信していから双方向通信により個別制御情報を配信する場合の処理動作を説明するためのフローチャート。
【図３８】本発明の第６の実施形態に係る情報配信装置の放送波にて電源オンコマンドパケットを配信していから双方向通信により個別制御情報を配信する場合の処理動作を説明するためのフローチャート。
【図３９】本発明の第６の実施形態に係る情報配信装置の共通制御パケットの送信処理動作について説明するためのフローチャート。
【図４０】本発明の第７の実施形態に係る情報配信装置の要部の構成例を示した図。
【図４１】コマンドパケットの作成処理動作について説明するためのフローチャート。
【図４２】双方向通信による個別制御パケットの送信処理動作について説明するためのフローチャート。
【図４３】双方向通信による個別制御パケットの送信処理動作について説明するためのフローチャート。
【図４４】本発明の第８の実施形態に係る情報配信装置の要部の構成例を示した図。
【図４５】図４４の情報配信装置の処理動作を説明するためのフローチャート。
【図４６】図４４の情報配信装置の処理動作を説明するためのフローチャート。
【符号の説明】
１００…限定受信部
１０１…モデム部

１０２…送受信部
１０３…マスター鍵格納部
１０４…個別制御情報復号部
１０５…ワーク鍵格納部
１０６…受信装置ＩＤ格納部
１０７…契約情報認証部
１０８…デジタル署名検証鍵格納部
１１１…放送波受信部
１１２…Ａ／Ｄ変換部
１１３…誤り検出／訂正部
１１４…チャネル選択部
１１５…チャネル選択インタフェース（Ｉ／Ｆ）部
１１６…フィルター部
１１７…共通制御情報復号部
１１８…チャネルキー格納部
１１９…チャネルキー出力部
１２０…デスクランブル部
１２１…契約情報格納部
１２２…契約判定部
１２３…チャネル情報入力部
２０２…加入者データベース
２０３…個別制御情報作成部
２０４…ワーク鍵データベース
２０５…デジタル署名生成鍵作成部
２０６…個別制御情報制御部
２０７…送受信制御部
２０８…モデム
２０９…共通制御情報作成部
２１０…ワーク鍵データベース
２１１…チャネルキーデータベース
２１２…共通制御情報制御部
２１３…放送送信制御部
２１４…放送送信部

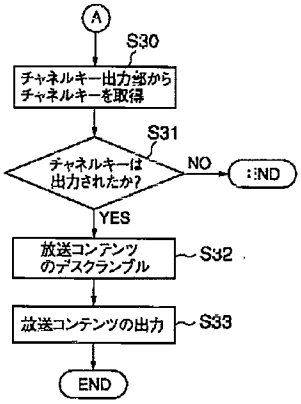
【図１】



【図２】



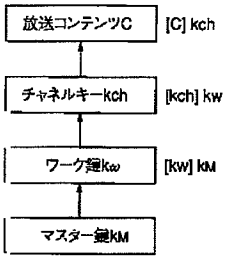
【図１１】

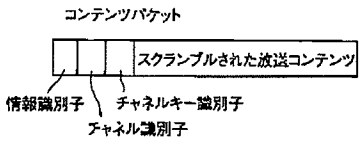


【図３】

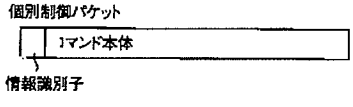
【図４】

【図６】

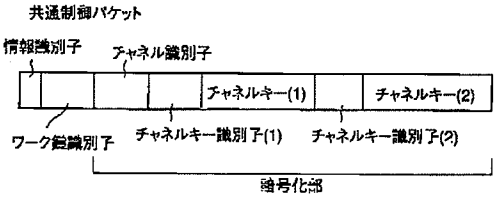




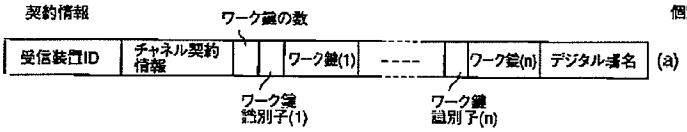
【図１６】



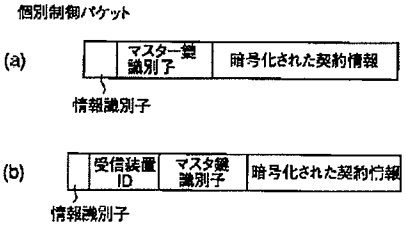
【図８】



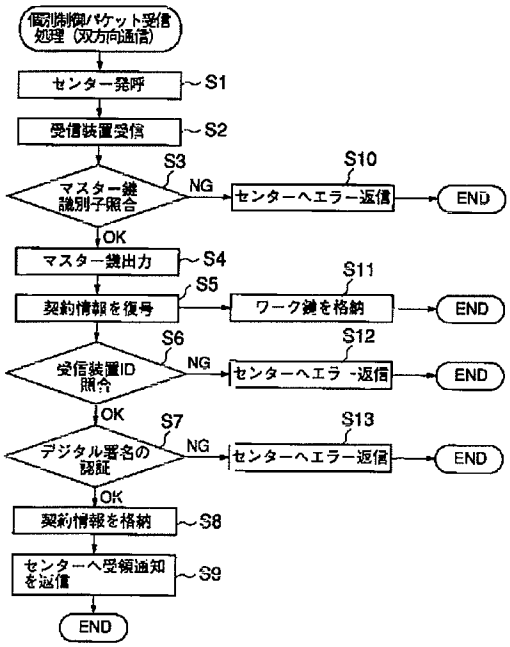
【図5】



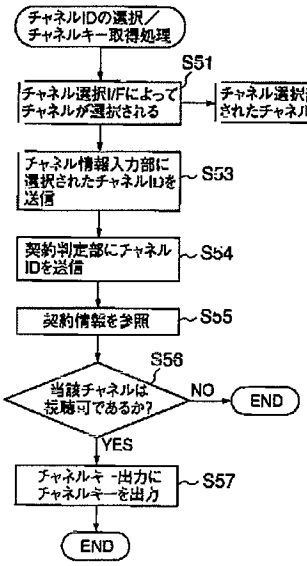
【図7】



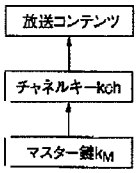
【図9】



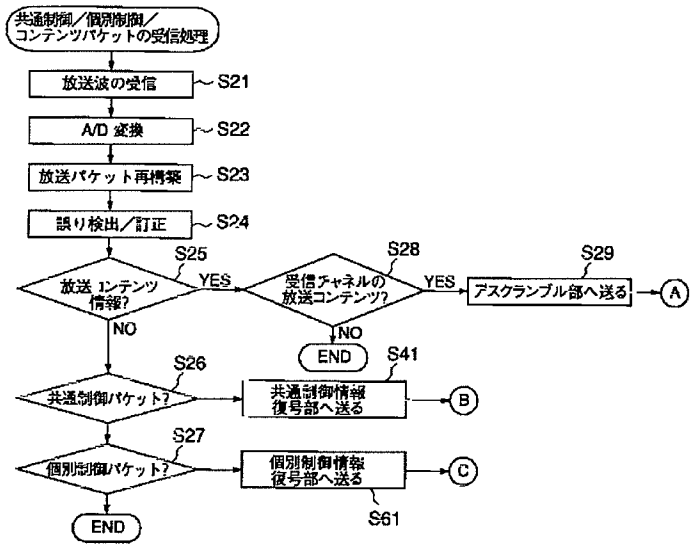
【図12】



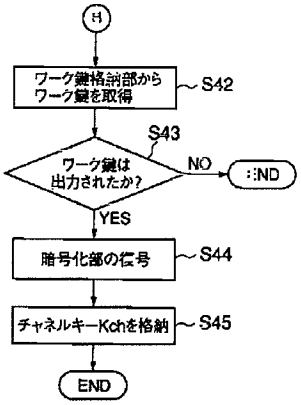
【図28】



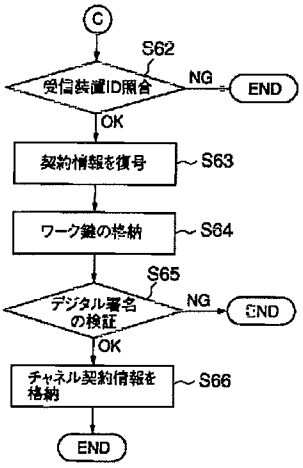
【図10】



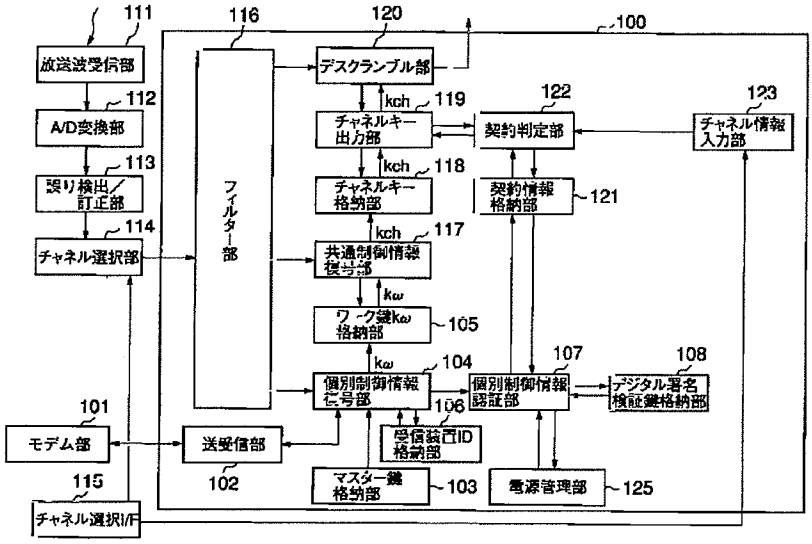
【図13】



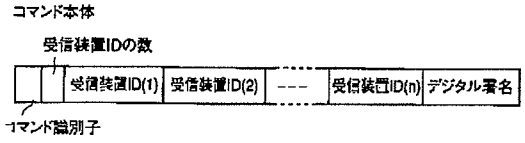
【図14】



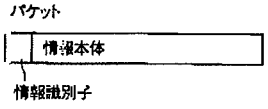
【図15】



【図17】

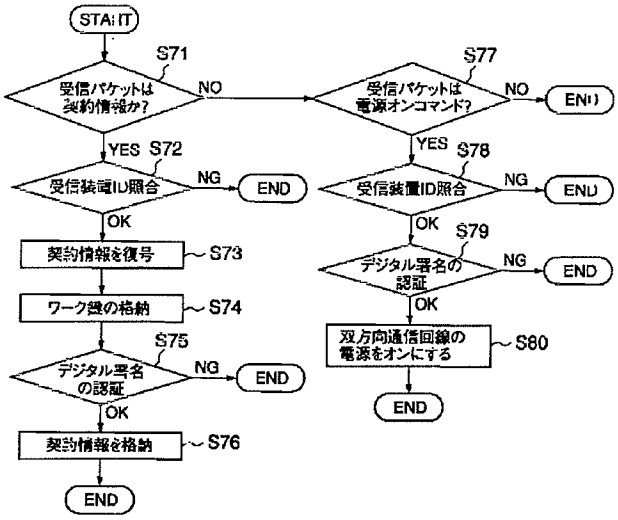


【図21】

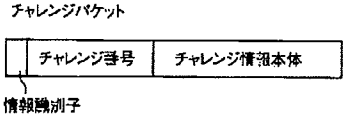


【図22】

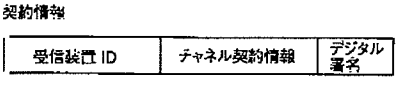
【図18】



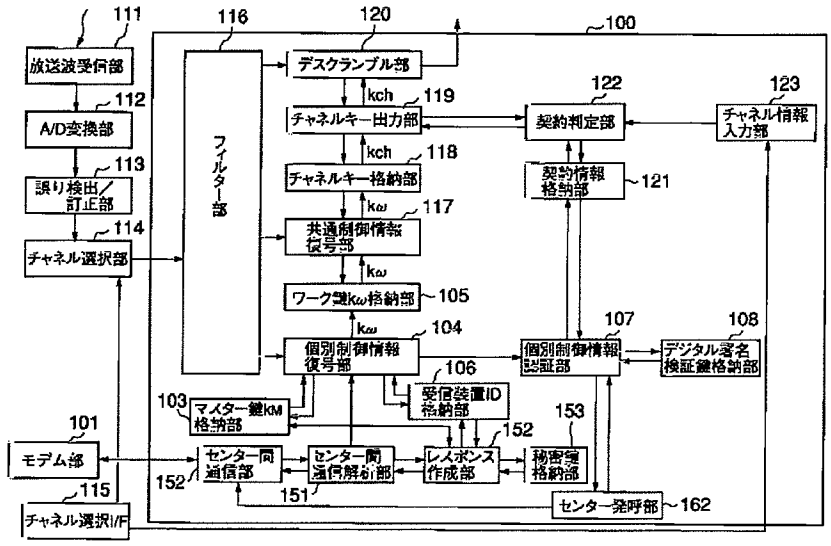
【図23】



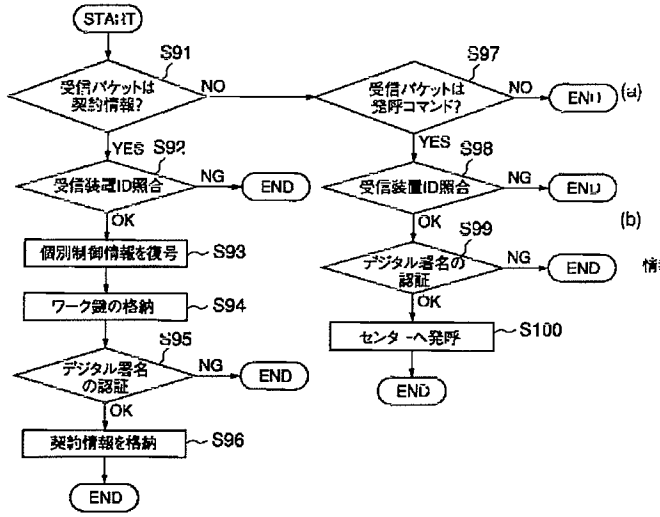
【図29】



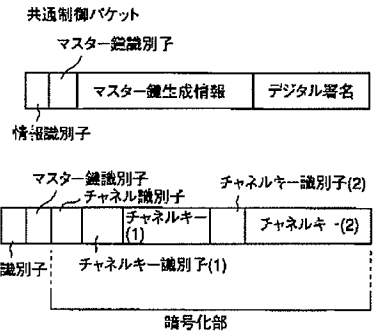
【図19】



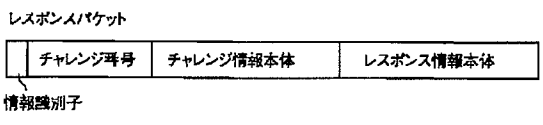
【図20】



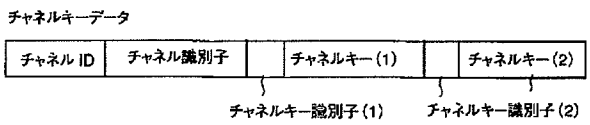
【図30】



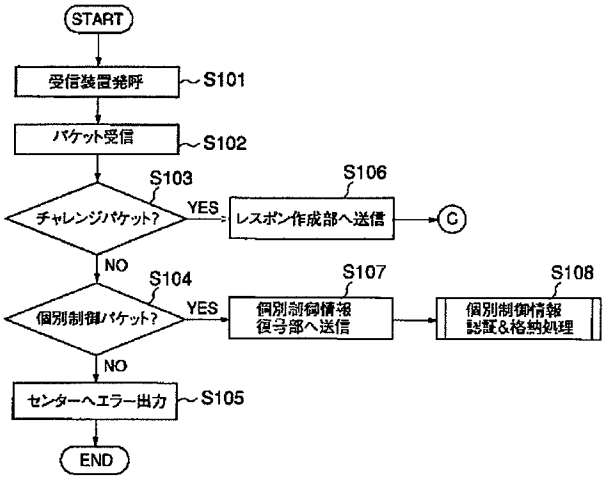
【図24】



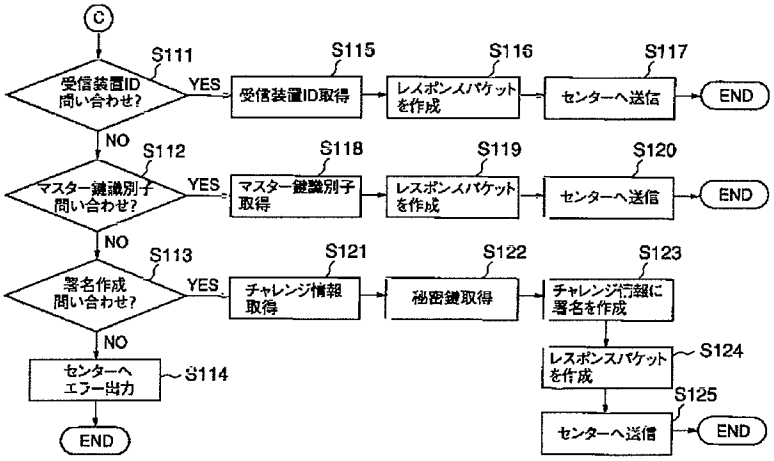
【図34】



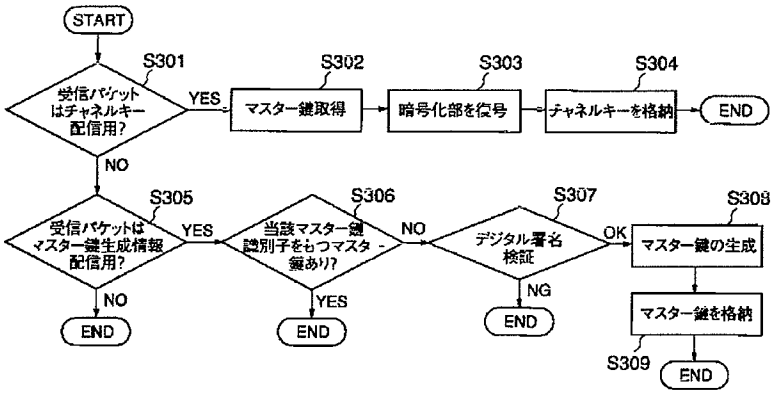
【図25】



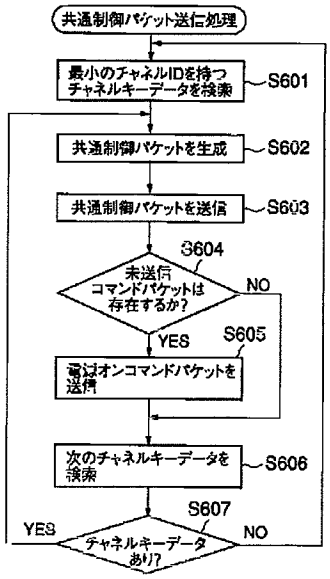
【図26】



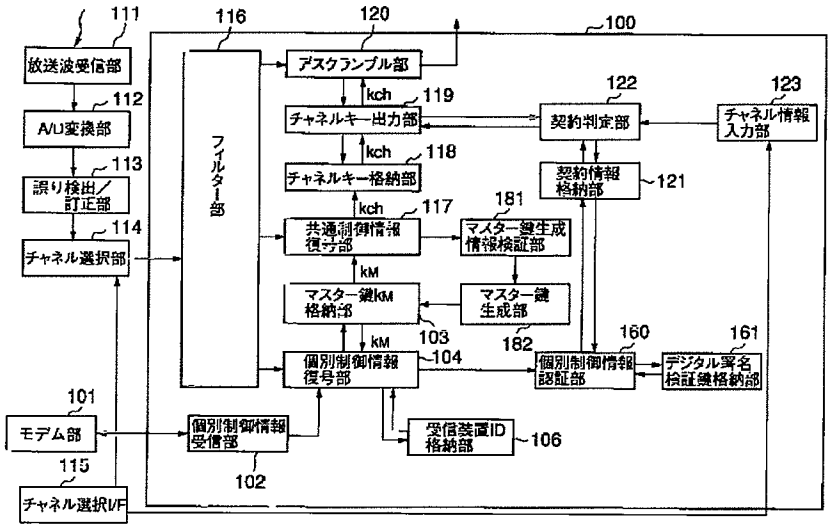
【図31】



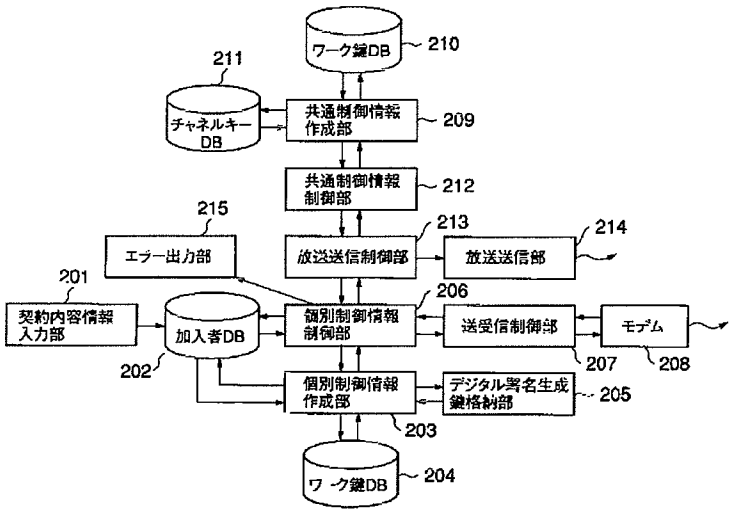
【図39】



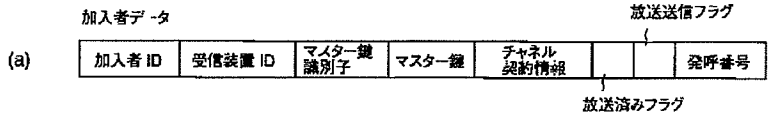
【図27】


111
116
120
100
放送波受信部
アスクランブル部
112
A/D変換部
kch
119
チャネルキー出力部
122
契約判定部
123
チャネル情報入力部
113
誤り検出訂正部
kch
118
チャネルキー格納部
契約情報格納部
121
114
チャネル選択部
フィルター部
kch
117
181
共通制御情報復号部
マスター鍵生成情報検証部
kM
マスター鍵KM格納部
マスター鍵生成部
182
160
161
kM
103
104
個別制御情報復号部
個別制御情報認証部
デジタル署名検証鍵格納部
101
モデム部
個別制御情報受信部
受信装置ID格納部
106
115
102
チャネル選択I/F

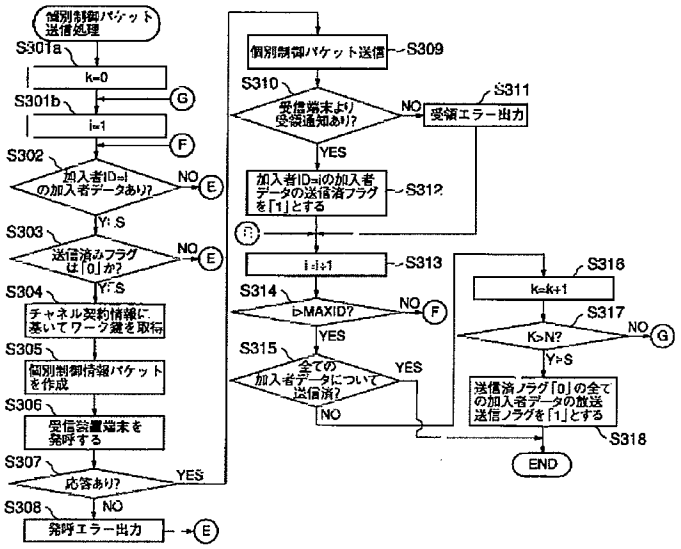
【図32】


ワーク鍵DB
210
211
チャネルキーDB
共通制御情報作成部
209
共通制御情報制御部
212
215
213
214
エラー出力部
放送送信制御部
放送送信部
201
206
契約内容情報入力部
加入者DB
個別制御情報制御部
送受信制御部
モデム
202
207
208
個別制御情報作成部
デジタル署名生成鍵格納部
205
203
ワーク鍵DB
204

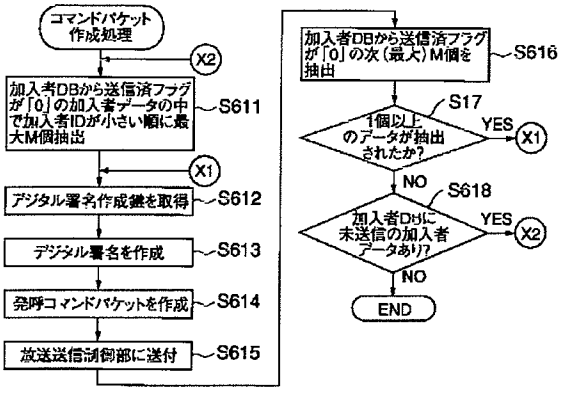
【図33】



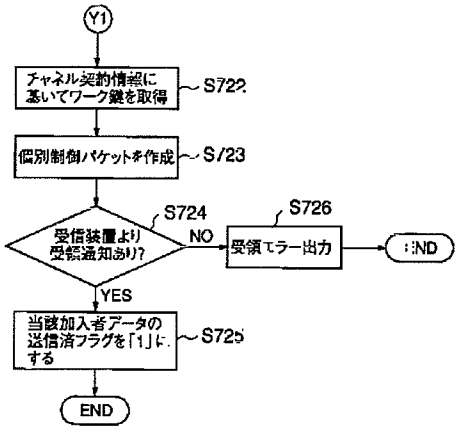
【図35】



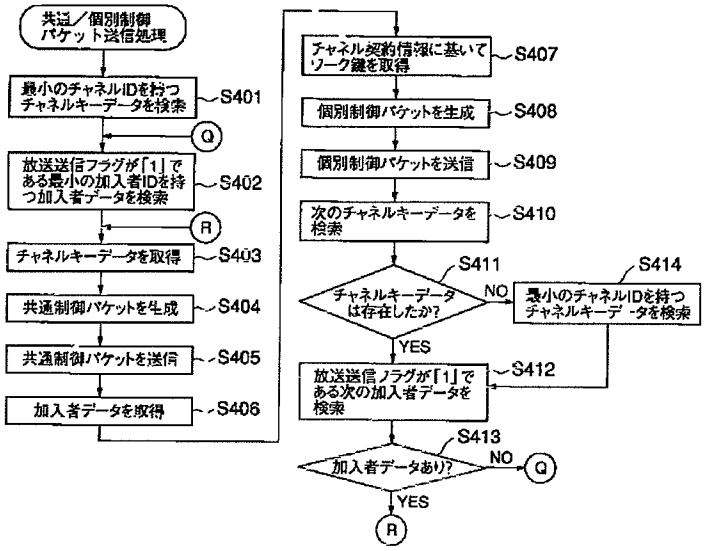
【図41】



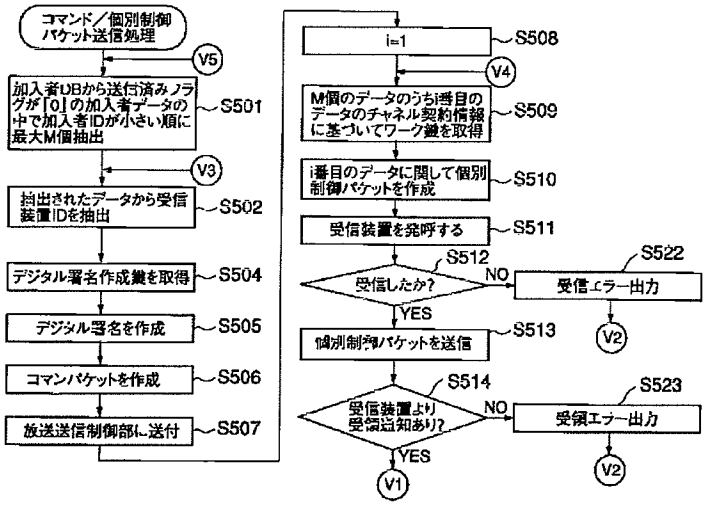
【図43】



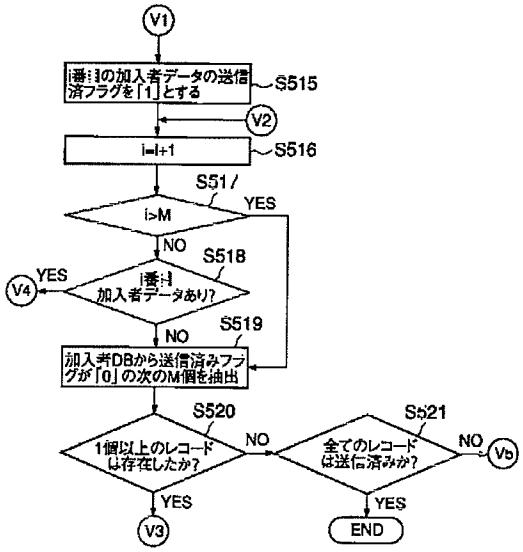
【図36】


共通／個別制御パケット送信処理
最小のチャネルIDを持つチャネルキーデータを検索
S401
Q
放送送信フラグが「1」である最小の加入者IDを持つ加入者データを検索
S402
R
チャネルキーデータを取得
S403
共通制御パケットを生成
S404
共通制御パケットを送信
S405
加入者データを取得
S406
チャネル契約情報に基いてワーク鍵を取得
S407
個別制御パケットを生成
S408
個別制御パケットを送信
S409
次のチャネルキーデータを検索
S410
S411
チャネルキーデータは存在したか?
NO
S414
最小のチャネルIDを持つチャネルキーデータを検索
YES
放送送信フラグが「1」である次の加入者データを検索
S412
S413
加入者データあり?
NO
Q
YES
R

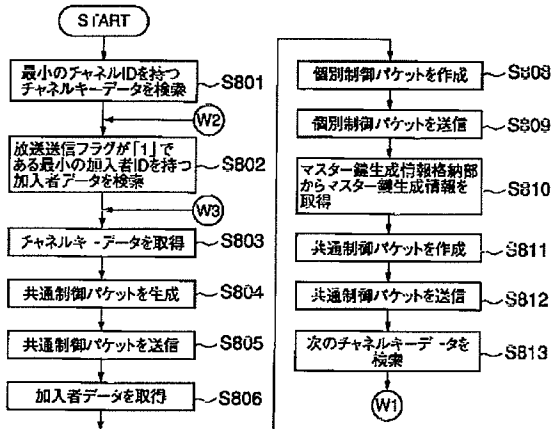
【図37】


コマンド／個別制御パケット送信処理
V5
加入者DBから送付済みフラグが「0」の加入者データの中で加入者IDが小さい順に最大M個抽出
S501
V3
抽出されたデータから受信装置IDを抽出
S502
デジタル署名作成鍵を取得
S504
デジタル署名を作成
S505
コマンドパケットを作成
S506
放送送信制御部に送付
S507
i=1
S508
V4
M個のデータのうちi番目のデータのチャネル契約情報に基づいてワーク鍵を取得
S509
i番目のデータに関して個別制御パケットを作成
S510
受信装置を発呼する
S511
S512
受信したか?
NO
S522
受信エラー出力
V2
YES
個別制御パケットを送信
S513
S514
受信装置より受領通知あり?
NO
S523
受領エラー出力
V2
YES
V1

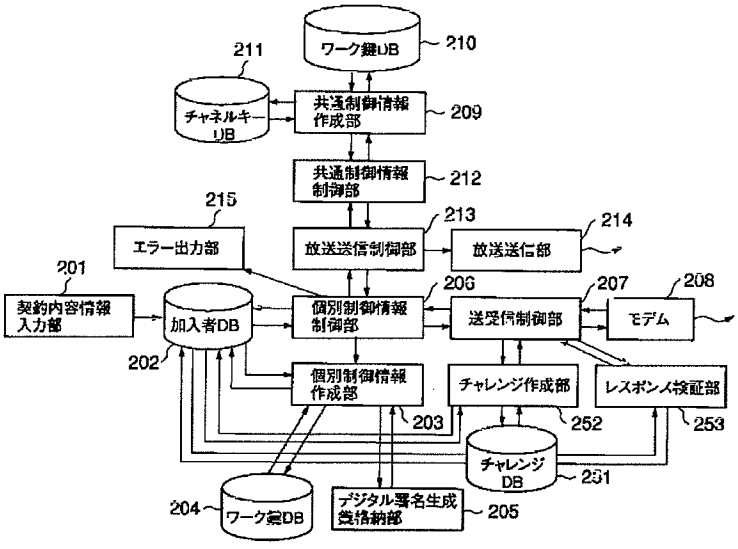
【図38】


V1
i番目の加入者データの送信済フラグを「1」とする
S515
V2
i=i+1
S516
S517
i>M
YES
NO
S518
i番目加入者データあり?
YES
V4
NO
S519
加入者DBから送信済みフラグが「0」の次のM個を抽出
S520
1個以上のレコードは存在したか?
NO
S521
全てのレコードは送信済みか?
NO
Vb
YES
V3
YES
END

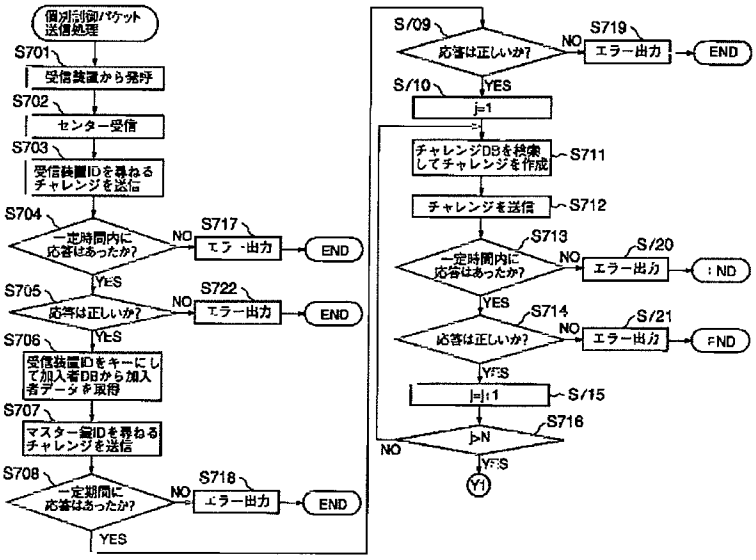
【図45】


START
最小のチャネルIDを持つチャネルキーデータを検索
S801
W2
放送送信フラグが「1」である最小の加入者IDを持つ加入者データを検索
S802
W3
チャネルキーデータを取得
S803
共通制御パケットを生成
S804
共通制御パケットを送信
S805
加入者データを取得
S806
マスター鍵格納部からマスター鍵を取得
S807
個別制御パケットを作成
S808
個別制御パケットを送信
S809
マスター鍵生成情報格納部からマスター鍵生成情報を取得
S810
共通制御パケットを作成
S811
共通制御パケットを送信
S812
次のチャネルキーデータを検索
S813
W1

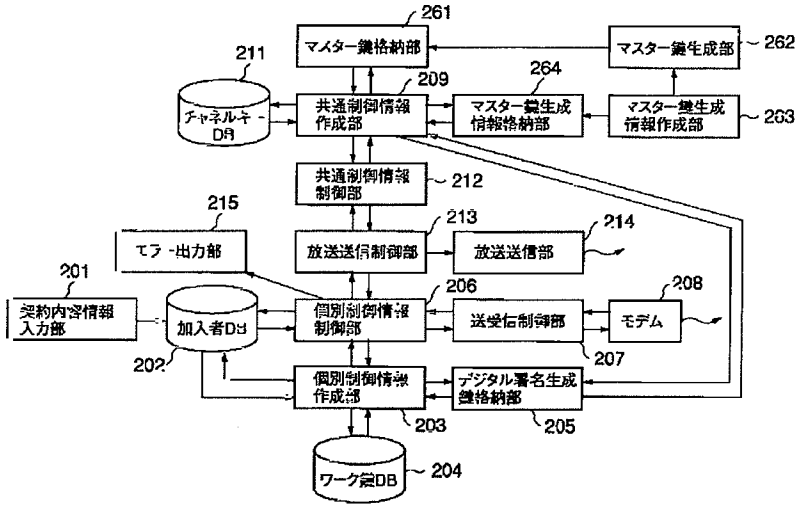
【図40】


ワーク鍵DB
210
211
チャネルキーDB
共通制御情報作成部
209
共通制御情報制御部
212
215
エラー出力部
213
放送送信制御部
214
放送送信部
201
契約内容情報入力部
加入者DB
202
206
個別制御情報制御部
207
送受信制御部
208
モデム
個別制御情報作成部
203
チャレンジ作成部
252
レスポンス検証部
253
チャレンジDB
251
204
ワーク鍵DB
デジタル署名生成鍵格納部
205

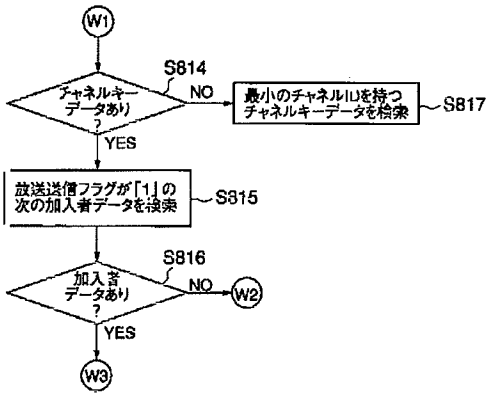
【図42】


個別制御パケット送信処理
S701
受信装置から発呼
S702
センター受信
S703
受信装置IDを尋ねるチャレンジを送信
S704
一定時間内に応答はあったか?
NO
S717
エラー出力
END
YES
S705
応答は正しいか?
NO
S722
エラー出力
END
YES
S706
受信装置IDをキーにして加入者DBから加入者データを取得
S707
マスター鍵IDを尋ねるチャレンジを送信
S708
一定期間に応答はあったか?
NO
S718
エラー出力
END
YES
S709
応答は正しいか?
NO
S719
エラー出力
END
YES
S710
j=1
チャレンジDBを検索してチャレンジを作成
S711
チャレンジを送信
S712
S713
一定時間内に応答はあったか?
NO
S720
エラー出力
END
YES
S714
必答は正しいか?
NO
S721
エラー出力
END
YES
j=j+1
S715
j>N
S716
NO
YES
Y1

【図44】


261
マスター鍵格納部
マスター鍵生成部
262
211
チャネルキーDB
209
共通制御情報作成部
264
マスター鍵生成情報格納部
マスター鍵生成情報作成部
263
共通制御情報制御部
212
215
エラー出力部
213
放送送信制御部
214
放送送信部
201
契約内容情報入力部
加入者DB
206
個別制御情報制御部
送受信制御部
208
モデム
207
202
個別制御情報作成部
203
デジタル署名生成鍵格納部
205
ワーク鍵DB
204

【図46】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
		H04N 7/167	Z	

Fターム(参考) 5C026 EA07
5C064 BA01 BB02 BC17 BC22 BD05
BD08 BD09 BD11 CA14 CB06
CC04
5J104 AA01 AA09 AA16 BA03 EA01
EA07 EA17 EA26 LA06 NA03
PA05

JP 2002-016565 PAJ machine translation

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a paid broadcasting system, for example.
[0002]
[Description of the Prior Art]Much more substantial service is expected as digital broadcasting starts in a communications satellite (CS) and digitization progresses to a cable TV and terrestrial broadcasting.
It seems that the leading role of broadcast service is played at future.

[0003]Can aim at improvement in the utilization ratio of the frequency which transmission of a program takes by introducing information-compression art, the steep increase in the number of broadcasting channels is attained as compared with analog broadcasting, and the greatest features of digital broadcasting are things. Since advanced error correction technique is applicable, offer of quality and homogeneous service is attained.
[0004]Not only in broadcast with a picture or a sound like before by digitization, It becomes possible for the broadcast (data broadcasting) by a character or data to also be attained, for example, to pass news as alphabetic data, or to distribute PC software by broadcast, and the system for providing such service is also appearing one after another. A receiving set and mobile type receiving sets, such as a Personal Digital Assistant which can be used not only a non-portable type like before but in movement, and a moving terminal currently installed by the car on the assumption that use in a car, have appeared.
[0005]When realizing paid broadcasting service in such a system, broadcast contents must be enciphered, it must transmit and customer relations management adapted to a contract term and contractual coverage must be able to be performed, such as solving scramble based on contractual coverage. For example, the customer relations management adapted to a contract term makes a program possible at a contract channel [within the contract term a contract of was made by the payment of the predetermined fee].
[0006]Moreover (based on a contract channel and a contract term), it is necessary to certainly provide only a just televiewer with the key information for solving scramble or a code with a receiving set also from a viewpoint of preventing unjust viewing and listening.
[0007]In order to realize this, conventionally, the contract information which showed the contract form including the channel information etc. in which the work key of the channel which prepares a master key and is carrying out the receiving contract to the televiewer who is doing the receiving contract and viewing and listening are possible was enciphered with the master key for every broadcast receiving set, and it had transmitted by the broadcast wave. A work key is a key peculiar to a channel, and can decode here the channel key of the channel concerned enciphered and sent. It is used for a channel key descrambling scramble (enciphered) contents (decoding).
[0008]In such a restricted reception system, it can be said that the work key and contract information which are enciphered with a master key (set up for every receiving set) are limited reception information peculiar to a receiving set, and the channel key enciphered with the work key (it is common to two or more receiving sets) is common limited reception information.
[0009]Even if it was peculiar limited reception information conventionally (it is unsuitable for

transmitting characteristic data), it had transmitted by the broadcast wave. since this cannot acquire the information on whether not only monopolizing the transmission band superfluously since the information to an individual member is transmitted to all the members but the member received, either, it is required -- period repeating transmission needed to be carried out.
[0010]The work key contained in individual limited reception information is set to every contract term (usually one month), Since the contract-management center side did not know whether limited reception information must be individually sent from a broadcasting station for every period of the, and also the receiving set actually received, if fixed time repeating transmission was not carried out, it cut in ****. For this reason, the rate of the individual limited reception information occupied to the present limited reception information is large fairly.
[0011]In order to solve this problem, two-way communication functions, such as a telephone line, are given to a receiving set, and how to transmit the limited reception information according to each receiving set individual by a bidirectional circuit, and transmit common limited reception information, including a channel key etc., by a broadcast wave etc. can be considered. However, since the bidirectional circuit is not indispensable in the present broadcasting industry (reception of usually broadcast sake), it will become impossible to use the aforementioned method on condition of a bidirectional circuit to no members for the reason of some members not owning the bidirectional circuit for limited reception. When the cellular phone etc. which can be desorbed are used as a bidirectional circuit, there is a problem that it cannot transmit since it is not connected at the time of limited reception transmitting information (under situation of any kind).
[0012]On the other hand, when transmitting limited reception information by a bidirectional circuit, call origination of the receiving set is carried out from the contract-management center now. By carrying out call origination from a receiving set, this is for avoiding that the stage of call origination laps and a circuit gets confused. However, for this reason, call origination of the center side must always be carried out, and there is a problem that communication charges start. When using a cellular phone as a bidirectional circuit like a mobile receiving set, in order always to have to change a cellular phone into the state waiting for mail arrival, there is a problem that there are many amounts of consumption of a power supply (since there is no telling when call origination occurs from a center).
[0013]
[Problem(s) to be Solved by the Invention]Thus, if the information which should be distributed to each addressing to a member with the increase in a member increased and the conventional conditional access system carried out broadcast distribution of them, it had the problem that broadcast bands will be pressed.
[0014]. Even though it distributes to each addressing to a member in two-way communication, such as a telephone network, a receiver does not have such a reception means. . Or a communication line cannot be connected when a receiver is power OFF. Or since it was necessary to perform call origination frequently, the burden of the communication charges of the transmitting side became large, or in a receiver, since it was necessary always to change into the state waiting for mail arrival, power consumption increased, and there was a problem of not being suitable for mobile environment.
[0015]Then, an object of this invention is to provide the information distributing device and broadcast receiving set using the information distribution method and it which enable offer of the paid broadcasting service with high safety which can prevent unjust viewing and listening, without pressing broadcast bands in view of such the actual condition, even if members increase in number.
[0016]

[Means for Solving the Problem]An information distribution method and a device of this invention receive enciphered contents information by which broadcast distribution was carried out, Are a receiving set which decodes contents information which can be decoded, and for decoding of said contents information. As opposed to a receiving set which decodes said contents information by which broadcast distribution was carried out based on key information required in order to decode decoding control information including information peculiar to said required receiving set, and said contents information independent of said receiving set, Carry out broadcast distribution of said key information, and individual control information for updating a part or all of said decoding control information that is memorized by said receiving set is distributed by two-way communication with said receiving set, In that case, when receipt of said individual control information on this receiving set is not checked, broadcast distribution of this individual control information is carried out.

[0017]According to this invention, individual control information according to each receiving set individual is distributed for key information common to all the receiving sets by two-way communication, such as a telephone line, by broadcast, Offer of paid broadcasting service with high safety which can prevent still more unjust viewing and listening is enabled without pressing broadcast bands by distributing a lot of individual control information, even if members increase in number since broadcast distribution of this individual control information is carried out when receipt of this individual control information is not able to be checked. Since distributing individual control information by two-way communication, such as a telephone line, can also be distributed by a broadcast wave, Decoding control information stored in a receiving set when a change of a channel to which it views and listens etc. are made (at the time of renewal of a contract). When updating (for example, channel contract information, a work key, etc.), about a receiving set connected to a two-way communication circuit, individual control information is transmitted by positive two-way communication, and when not connected under a certain situation, individual control information can be transmitted by a broadcast wave. That is, individual control information can be certainly distributed to a member.

[0018]By carrying out call origination of said receiving set, and distributing said individual control information by said two-way communication, after carrying out broadcast distribution of the command for changing said receiving set into a state waiting for mail arrival preferably, While being able to attain power-saving of a receiving set since the receiving set is changed into a state waiting for mail arrival only when distributing individual control information, individual control information can be distributed certainly and a paid broadcasting system suitable for mobile environment can be provided.

[0019]By carrying out broadcast distribution of the command which directs call origination from said receiving set preferably in order to distribute said individual control information by said two-way communication, even if it is a case where it is alike by call origination from the receiving set side, and individual control information is distributed, By managing generating timing of call origination by the information distributing device side, a situation where a circuit is not connected easily and becomes an information distributing device is avoidable by, for example, concentrating on a time zone with call origination from a receiving set.

[0020]preferably, after attesting said receiving set, even if it is a case where it is alike by call origination from the receiving set side, and individual control information is especially distributed by distributing said individual control information by two-way communication, distribution of individual control information is attained safely.

[0021]There is the same effect as the above also by enciphering and carrying out broadcast distribution so that said key information can be decoded by other key information generated by

said receiving set based on key creation information by which broadcast distribution is carried out.

[0022]In a broadcast receiving set which a broadcast receiving set of this invention receives enciphered contents information by which broadcast distribution was carried out, and decodes contents information which should be decoded, A memory measure which memorizes decoding control information including information peculiar to a self-device required for said decoding of contents information by which broadcast distribution was carried out, Two-way communication distributes from the 1st distribution system that distributes individual control information for updating a part or all of decoding control information that was memorized by this memory measure, Or when two-way communication receives individual control information addressed to a self-device by the 1st reception means that receives individual control information addressed to a self-device by which broadcast distribution was carried out from said 1st distribution system, and this 1st reception means, A receipt transmitting means which transmits that receipt to said 1st distribution system, and an update means which updates decoding control information memorized by said memory measure based on individual control information received by this 1st reception means, The 2nd reception means that receives said key information by which broadcast distribution was carried out from the 2nd distribution system that distributes key information common to said all broadcast receiving sets required in order to decode said contents information, Said contents information by which broadcast distribution was carried out is decoded based on decoding control information memorized by said memory measure and key information received by said 2nd reception means.

[0023]According to this invention, when each broadcast receiving set receives key information common to all the receiving sets by broadcast two-way communication, such as a telephone line, or when it carries out two-way communication and cannot receive, and it receives individual control information according to each receiving set individual by broadcast, Offer of paid broadcasting service with high safety which can prevent still more unjust viewing and listening is enabled without pressing broadcast bands by distributing a lot of individual control information, even if members increase in number. Since distributing individual control information by two-way communication, such as a telephone line, can also be distributed by a broadcast wave, Decoding control information stored in a receiving set when a change of a channel to which it views and listens etc. are made (at the time of renewal of a contract). When updating (for example, channel contract information, a work key, etc.), a receiving set connected to a two-way communication circuit receives individual control information by two-way communication, and when not connected under a certain situation, it can receive individual control information by a broadcast wave. That is, each receiving set can receive individual control information certainly.

[0024]By changing a self-device into a state waiting for mail arrival so that a command by which broadcast distribution was carried out may be received preferably and said individual control information distributed from said 1st distribution system can be received, While being able to attain power-saving of a receiving set since what is necessary is just to change into a state waiting for mail arrival only when receiving individual control information, individual control information can be distributed certainly and a receiving set suitable for mobile environment can be provided.

[0025]By carrying out call origination of said 1st distribution system, in order to receive preferably a command by which broadcast distribution was carried out and to receive said individual control information, even if it is a case where it is alike by call origination from the receiving set side, and individual control information is received, By managing generating timing of call origination by the distribution system side of ** 1st, a situation where a circuit is not

connected easily and becomes a center (the 1st distribution system) is avoidable by, for example, concentrating on a time zone with call origination from a receiving set.
[0026]preferably, after a self-device is attested from said 1st distribution system, even if it is a case where it is alike by call origination from the receiving set side, and individual control information is especially received by receiving said individual control information, distribution of individual control information is attained safely.
[0027]There is the same effect as the above also by enciphering that said key information can be decoded by other key information generated based on key creation information received separately.
[0028]
[Embodiment of the Invention]Hereafter, the embodiment of this invention is described with reference to drawings.
[0029]First, a definition of term is performed. It names generically permitting viewing and listening of broadcast contents only to the limited person (it is hereafter called a regular contractor, a member, or a user) who gave encryption etc. and performed predetermined contract / subscription procedure etc. when receiving the broadcast contents which consist of one or more channels, and it is called limited reception. The system which realizes limited reception is named generically and it is called a conditional access system. This embodiment explains taking the case of the conditional access system for paid broadcasting service, for example.
[0030]In order to perform limited reception, the information which described the contract condition for every channel for every member is called channel contract information. For example, the bit string which attached the channel designator to each channel and expressed the contract condition of the channel by whether the bit corresponding to a channel designator is "1" like drawing 2 is channel contract information. Drawing 2 shows that a contract of the 2nd, the 5th, the 7th, and the 8th channel is made.
[0031]As shown in drawing 6, the information which adds restriction to channel contract information, such as the term of validity of the channel contract information concerned, and the information which expresses a member's contract form in details more are added to the channel contract information shown in drawing 2, and channel contract information may be constituted.
[0032]Each subscriber to the paid broadcasting service concerning this embodiment differs in contractual coverage (a channel to view and listen, the period to which it views and listens), respectively. That is, in order to make possible limited reception to the broadcast receiving set which these members possess, it is necessary to distribute individually the control information on the broadcast receiving set concerned based on different contractual coverage (utilization condition) for every member. Such control information is called individual control information. Since individual control information is distributed by packet format, it is also called an individual control packet in that case. EMM [in / for example / in this individual control packet / the present CS broadcasting standard] (Entitlement Management Message), It hits EMM-S (Entitlement Management Message for S-band) (reference "BS-digital-broadcasting restricted reception system standards ARIB STD-B25 (Association of Radio Industries and Businesses)").
[0033]Broadcast contents information (it may be hereafter called contents simply) is enciphered by the "channel key" at different key information for every channel, i.e., here. Therefore, in order to view and listen to the contents of a desired channel (it contracted) with the broadcast receiving set which each member possesses, it is necessary to also distribute control information common to all the members (all the broadcast receiving sets which a member possesses) like the key information depending on this contents information. Such control information is called common control information. Since common control information is also distributed by packet format, it is

also called a common control packet in that case. ECM [in / for example / in this common control packet / the present CS broadcasting standard] (Entitlement Control Message), It hits ECM-S (Entitlement Control Message for S-band) (reference "BS-digital-broadcasting restricted reception system standards ARIB STD-B25 (Association of Radio Industries and Businesses)".).
[0034]When the broadcast receiving set which each member possesses receives individual control information and common control information certainly, viewing and listening of contents information in alignment with each member's contractual coverage is attained.
[0035]The composition (mainly hardware) which realizes the limited reception method inside a receiving set is called a limited reception part or limited reception chip through following embodiments. Since the confidential information for limited reception was contained in the limited reception chip, it read easily from the exterior about an internal memory and hard structure, and the Tampa-proof structure which cannot perform writing and change is assumed. The television television machine for actually reproducing contents information decoded by this set top box in the set top box concerned, such as a sound and an image, radio, etc. may be connected by making a limited reception part into a set top box, and a broadcast receiving set may be constituted as a whole.
[0036]In the following explanation, it may call it descrambling to decode the enciphered contents information using a channel key.
[0037]The conditional access system explained by following embodiments, It mainly comprises a broadcast receiving set which a service subscriber possesses, and an information distributing device (contract-management device) as a contract-management center (it may be simply called a center) which distributes individual control information, common control information, encrypted contents information, etc. to this broadcast receiving set.
[0038](A 1st embodiment) A 1st embodiment of this invention is an embodiment in the conditional access system which has a master key with each individual receiving set. Since such a conditional access system must encipher the control information which includes channel contract information etc. periodically and individually and must transmit, it has the problem that a transmission amount becomes large. On the other hand, since safety is high, it has been adopted by CS broadcasting and others from the former that the damage range at the time of a master key being torn is narrow etc. However, the quantity of the control information which should be sent according to a receiving set individual is becoming huge with the increase in a member in recent years, and this embodiment gives this solution.
[0039]In such a conditional access system, key composition as shown in drawing 3 is adopted, for example. That is, the work key Kw common to all the receiving sets defined for every channel is enciphered with the master key KM according to each receiving set individual, and it transmits. Using the work key Kw, the channel key Kch is enciphered and it transmits. Since broadcast contents are enciphered with the conventional encryption system using the channel key Kch, it can decode by this channel key. A channel key must usually be changed in a short time for about 10 minutes here in order to prevent a decipherment. A transmission amount becomes huge, if the individual master key was used in order to transmit this. Therefore, it is necessary to use a work key common to all the receiving sets. Since a work key is also dangerous if the same key is used in the unit of how many months, it is necessary to change and it serves as structure which enciphers this with an individual master key. Even if a metaphor master key is known by this, by it, free viewing and listening can be prevented by changing a work key.
[0040]Now, the data which the broadcast receiving set used for the conditional access system of a 1st embodiment receives from a broadcast wave is three kinds, a contents packet, a common control packet, and an individual control packet.

[0041]The contents packet consists of an information identifier, a channel identifier, a channel key identifier, and broadcast (enciphered) contents by which scramble was carried out by the packet format shown in drawing 4. An information identifier describes the identifier which shows the classification of the packet concerned and shows that it is a contents packet here. As for a channel identifier, the broadcast contents concerned show of which channel they are contents. A channel key identifier shows the identifier of the channel key which decodes the broadcast contents concerned. Broadcast contents are raw program data and are enciphered by the channel key Kch specified by the channel key identifier. All the information (data) described by this embodiment shall be expressed by fixed length.
[0042]By the packet format which the common control packet explained here is a common control packet for channel key distribution, and is shown in drawing 8. An information identifier, a work key identifier, a channel identifier, a channel key identifier (1), It comprises a channel key (1), a channel key identifier (2), and a channel key (2), and the portion from a channel identifier to a channel key (2) is enciphered with the work key shown by the work key identifier. An information identifier describes the identifier which shows the classification of the packet concerned and shows that it is a common control packet (common control packet for channel key distribution) here. As for a channel identifier, the common control packet concerned shows which channel thing it is. A work key identifier is information which shows by which work key Kw the common control packet concerned is enciphered. A channel key identifier is an identifier of the channel key described below, and the channel key shows the channel key currently used for encryption of the broadcast contents of the channel specified by the channel identifier.
[0043]It is because a channel key is changed comparatively for a short time, so that a channel key identifier and 2 sets of channel keys exist has sent simultaneously the channel key used from the necessity of changing a channel key smoothly now, and the channel key used next time as mentioned above here. Of course, since direct influence is not carried out to this invention, it may be 1 set that 2 sets transmits in this way.
[0044]two kinds in the case of the case where individual control information is distributed via a modem in this embodiment from the two-way communication circuit which used the public network (telephone network) etc., and a broadcast wave distributing -- it is . Anyway, although individual control information as well as common control information is transmitted by packet format and there is no change in things, the form has a difference a little.
[0045]The individual control packet transmitted by a two-way communication circuit is an individual control packet for contract information distribution of composition as shown in drawing 7 (a), and consists of an information identifier, a master key identifier, and enciphered contract information. An information identifier shows the classification of the packet concerned and describes here the identifier which shows that it is an individual control packet for contract information distribution. A master key identifier is the identification information of the master key which can decode the individual control packet concerned, and if transmitted and received correctly, the master key identifier which the receiving set which should receive the packet concerned has is described here.
[0046]The individual control packet by which broadcast distribution is carried out is same individual control packet for contract information distribution, and as shown in drawing 7 (b), it differs from the individual control packet (refer to drawing 7 (a)) to which the point that receiving set ID is added to an unenciphered portion is transmitted by two-way communication. This receiving set ID is the information which shows of which addressing to a receiving set the individual control packet concerned is a thing, and since it differs in a master key (this packet is decoded) the whole receiving set, it is indispensable information.

[0047]As shown in drawing 5, it is contract information from the pair of several n and n work keys of receiving set ID, channel contract information, and a work key, and a work key identifier, and the digital signature. Receiving set ID is an identifier of a receiving set which should receive the contract information concerned, and if it is transmitted and received normally, it is receiving set ID in the limited reception part 100 inside a receiving set, and congruous ID. Channel contract information shows the channel which can receive the receiving set which has the receiving set ID concerned, and as shown in drawing 6, it consists of channel contract information and its term of validity here, for example. Work key identifier (i) is an identifier of continuing work key (i). Since the work key is set up for every channel in this embodiment, the group of the work key corresponding to channel contract information and a work key identifier enters. A digital signature is the information for checking the justification of the contract information (especially channel contract information) concerned, and is mainly used for forgery prevention.
[0048]By a 1st embodiment, since all these information is the data expressed by fixed length, the algorithm which extracts each information from the received packet is not described anew.
[0049]Next, the composition and processing operation of the broadcast receiving set (it may be hereafter called a receiving set simply) concerning a 1st embodiment are explained. Drawing 1 is what showed the example of composition of the important section of a broadcast receiving set, and it explains first the individual control packet reception operation by the two-way communication shown in drawing 9, referring to drawing 1.
[0050]The broadcast receiving set of drawing 1 is answering to the call origination from a center via the modem section 101, and the session for transmitting and receiving an individual control packet via the two-way communication circuit is established (Step S1). When an individual control packet as shown in drawing 7 (a) is received and the packet concerned recognizes that it is for contract information distribution from the information identifier, the transmission and reception section 102 passes it to the individual control information decoding part 104, and here, A master key identifier is acquired from the packet concerned (Step S2, Step S3). If the acquired master key identifier is not a master key identifier corresponding to the master key stored in the master key storing part 103, an error will be transmitted to a center using the session established (Step S3, Step S10). When it is the corresponding master key identifier (Step S3), the contract information included in the packet which received is decoded using the master key concerned outputted from the master key storing part 103 (step S4) (Step S5).
[0051]The work key contained in the decoded contract information and its identifier are stored in the work key storage 105 (Step S11). Receiving set ID contained in the contract information concerned is compared with receiving set ID stored in the receiving set ID storage 106, and if not in agreement, an error is outputted to a center via the transmission and reception section 102 (Step S6, Step S12). If in agreement, the key information stored in the digital signature verification-keys storage 108 by the contract information authentication section 107 will be used (for example, channel contract information.). Or portions other than a digital signature are enciphered by the key information concerned among the contract information shown in drawing 5, If the digital signature of the contract information concerned is verified (Step S7) and verification is not successful by comparing the result and the digital signature in contract information, the error reply of that is carried out to a center via the transmission and reception section 102 (Step S13).
[0052]If verification is successful, after storing channel contract information in the contract information storage 121 (Step S8), the acknowledgment of receipt which shows that the renewal of contract information carried out normal termination is transmitted to a center, and it ends (step S9).

[0053]Here explains the verification processing of the digital signature in the contract information authentication section 107. A digital signature here is roughly divided and is considered two. Then one used the common key encryptosystem, it is a method which exists, has a center, a cryptographic algorithm common to a receiving set, and a common secret key, enciphers contract information sequentially by a block unit with the secret key of this **, and makes the last block a digital signature. Successive encryption is a method of encryption with which a pre- block affects encryption of the present block here. For example, the present block is enciphered with a secret key and it can realize by considering it as the encryption result of the present block with the exclusive OR of the encryption result and the encryption result of a pre-block. Even when this method was used and an intermediate block is altered, since a different (in the cases of most) digital signature is generated, it becomes alteration detection.
[0054]Always the ability to perform signature verification by a common key encryptosystem at high speed To a digital signature, the characteristic quantity of the whole data called a hash value besides said technique to sign is calculated, and the technique of enciphering the value is known again. A hash value is calculated from the whole data, and when at least 1 bit of data is changed, there is the feature that it is difficult to create data with that hash values differ remarkably and the same hash value. Alteration detection is attained for such character. A hash value is created by a hash function with fixed length data.
[0055]Although it does not come out, and circuit structure is small and ends, since a receiving set has the same information as a center, there is the feature that it is weak in hacking etc.
[0056]Another is the method which used public key encryption, and verifies by a public key what signed with the secret key. Since it is very difficult here to derive a secret key from a public key, even if a receiving set is hacked and it extracts a public key, it is the feature for an alteration to be fairly difficult. Although it is a method with very high safety, there is also a weak point where it being not only a low speed but circuit structure becomes large.
[0057]With the character which was excellent in such a digital signature, it can be said that the receiving set is carrying out information distributing device (leading digital signature added to individual control packet) (it is also called contract-management device) attestation. However, a digital signature is not indispensable in order to solve the problem considered by this invention. That is, this invention can be carried out that a digital signature is not indispensable in the individual control packet of this invention, and the composition excluding the digital signature from the individual control packet does not have inconsistency, either.
[0058]Next, with reference to the flow chart shown in drawing 10 - drawing 14, the broadcast receiving set of drawing 1 explains the processing operation which receives common control information, contents information, and common control information from a broadcast wave. If a receiving set receives the broadcast wave sent from the center in the broadcast receive section 111 and an electrical signal is acquired (Step S21), it will change it into a digital signal from an analog signal in the A/D conversion part 112, and will change it into packet format digital data (Step S22, Step S23). After being sent to error detection / correction part 113 and performing predetermined error detection/correction (Step S24), digital data distinguishes individual control a contents packet, a common control packet, or a packet with reference to the information identifier of the receive packet concerned, branches according to it, and advances processing.
[0059]By the way, the channel identifier which the channel selection interface (I/F) 115 acquires the channel identifier under present viewing and listening, and was acquired here is passed to the channel selection part 114 and the channel information input part 123 (Step S51 - Step S53 of drawing 12).
[0060]When it is a contents packet, channel I/F115 is passed for (Step S25), the channel selection

part 114 passes the channel under present viewing and listening, it obtains and only the contents packet of a viewing-and-listening channel is passed to the filter part 116 of the limited reception part 100 based on this (Step S28). In the filter part 116, this is sent to the descrambling part 120 (Step S29).

[0061]On the other hand, when it is a common control packet, through (Step S26) and the channel selection part 114, it is sent to the common-control-information decoding part 117 by the filter part 116, and decoding is started (Step S41).

[0062]Next, the processing to a contents packet is explained in detail along with the flow chart of drawing 11. A channel identifier, a channel key identifier, and ** are separated from the contents packet sent to the descrambling part 120 at Step S29 of drawing 10, and they are passed to the channel key outputting part 119. The output of a channel key is demanded from the channel key outputting part 119 from the descrambling part 120.

[0063]The channel key outputting part 119 extracts the channel key of the reception channel under present viewing and listening from the channel key storage 118 based on the contract judging to the channel identifier concerned in the contract judgment part 112. Namely, as shown in drawing 12, the contract judgment part 122, Acquire the channel identifier of the channel to which it is viewed and listened now from the channel information input part 123 (Step S54), and channel contract information as shown in drawing 2 already memorized by the contract information storage 121 is referred to, If the bit corresponding to the acquired channel identifier is "1" and it is "permission" and "0", the signal of "disapproval" will be sent to the channel key outputting part 119 (Step S55). If the sent decision result is "permission" in the channel key outputting part 119, the channel key which has the channel key identifier taken out from the contents packet from the channel key storage 118 will be obtained from the channel key storage 118, The descrambling part 120 is passed (Step S57). If a decision result is "disapproval", the processing about the contents packet concerned will be ended there.

[0064]The descrambling part 120 will decode and output the enciphered contents information which is included in a contents packet using it, if a channel key is received from the channel key outputting part 119 (Step S31 - Step S33 of drawing 11).

[0065]Next, the processing to a common control packet is explained with reference to the flow chart shown in drawing 13. A common control packet is sent to the common-control-information decoding part 117 from the filter part 116 (Step S41 of drawing 10). Here, a work key is acquired from the work key storage 105 based on the work key identifier contained in the non-cryptopart of a common control packet (Step S42 of drawing 13). Processing is ended when a work key is not able to be acquired. If a work key is acquirable, the encryption section of a common control packet is decoded with the work key concerned (Step S44). The channel key Kch is acquired from the encryption section of the decoded common control packet, and it stores in the channel key storage 118 (Step S45).

[0066]Next, the processing to an individual control packet is explained with reference to the flow chart shown in drawing 14. An individual control packet is sent to the individual control information decoding part 104 from the filter part 116 (Step S61 of drawing 10). Here, receiving set ID is extracted from an individual control packet (non-encryption section), and it compares with receiving set ID of the self-device stored in the receiving set ID storage 106 (Step S62 of drawing 14). When extracted receiving set ID is not in agreement with it of a self-device, processing of this packet is ended. When in agreement, the master key identifier taken out from the receive packet (non-encryption section) concerned is used as a key, and a master key is acquired from the master key storing part 103. A work key and its identifier are taken out from the contract information (refer to drawing 5) which decoded the contract information in the

individual control packet concerned using the master key concerned (Step S63), and was acquired by decoding, and it stores in the work key storage 105 (Step S64).
[0067]Next, the decoded contract information is sent to the contract information authentication section 107. In the contract authentication section 107, since portions other than the digital signature of this contract information are stored in the digital signature verification-keys storage 108, encipher using digital signature verification keys and a digital signature is acquired, A digital signature is verified based on whether to be in agreement with the digital signature in the contract information concerned (Step S65). When verification is successful, the channel contract information in contract information is stored in the contract information storage 121, and processing is finished (Step S66). It ends without storing, since channel contract information may have been forged or it may have been destroyed by receiving [poor], when verification went wrong.
[0068]Since it is receivable by both the case where two-way communication, such as a telephone line, receives individual control information, and the case where what was distributed by the broadcast wave is received according to the broadcast receiving set concerning a 1st embodiment of the above as explained above, When a change of the channel to which it views and listens etc. are made (at the time of renewal of a contract) and the channel contract information etc. which are stored in the receiving set are updated, About the receiving set connected to the two-way communication circuit, an individual control packet is transmitted by positive two-way communication, and when not connected under a certain situation, an individual control packet can be transmitted by a broadcast wave.
[0069]Although a 1st embodiment showed only the composition of the broadcast receiving set (the information distributing device concerning a 1st embodiment) By distributing individual control information which is explained by a 5th embodiment and which was mentioned above by both two-way communication and broadcast, For example, even if it is a broadcast (it does not have modem section [of drawing 1] 101, and transmission and reception section 102) receiving set without two-way communication functions, such as a cellular phone, renewal of channel contract information can be ensured.
[0070](A 2nd embodiment), next some variations are described. The 1st variation precedes transmitting individual control information using a two-way communication circuit from a center, and transmits the command which makes one the power supply of the two-way communication function (for example, portable telephone function) by the side of a receiving set by a broadcast wave.
[0071]By doing in this way, it becomes unnecessary to always change the receiving set side into a power turn state (mail arrival waiting state) for the individual control information which is not understood when it receives a message, and it can realize power saving. In the mobile environment which uses a cell as the main power supplies, realization of such power saving is important.
[0072]Although the composition of the important section of the broadcast receiving set concerning a 2nd embodiment is shown in drawing 15, In drawing 15, although it corresponds after the transmission and reception section 102 and the modem section 101, since this invention has the feature in a limited reception part, the detailed composition and its explanation of a two-way communication function part are omitted, and only the composition concerning the operation which performs the power turn/OFF control of the function is explained to be a two-way communication function. For example, a cellular phone can be connected to the transmission and reception section 102 using a predetermined connecting cable, and a two-way communication function part can also be constituted.

[0073]In drawing 15, the formation part about the reception of the individual control packet which transmits by a broadcast wave differs from a 1st embodiment. Since the receiving procedure of a common control packet is the same as a 1st embodiment, below, it actually stops to explain only the composition and reception operation of a different point, i.e., the individual control packet which receives from a broadcast wave.
[0074]In a 2nd embodiment, the individual control packet received by a broadcast wave is two kinds such as the thing for contract information distribution, and the thing for command distribution. Since the individual control packet for contract information distribution is the same as the thing (refer to drawing 7 (b)) of a 1st embodiment, here explains only the individual control packet for command distribution (it may be hereafter called a command packet).
[0075]The command packet consists of an information identifier and a command main part, as shown in drawing 16. As a command main part is roughly divided and it is shown in drawing 17, only in the command identifier, the number, and the number of receiving set ID of receiving set ID, receiving set ID is located in a line, and a digital signature continues after that. A digital signature is attached to the number of receiving set ID, and the row of receiving set ID for forgery prevention. A command identifier here is a command identifier for identifying always that it is a "power turn" command for starting supply of the power supply to the two-way communication function of the broadcast receiving set for changing into (the state waiting for mail arrival) in the state in which receipt is possible. Hereafter, the command packet which distributes a "power turn" command is called a power turn command packet.
[0076]Drawing 18 is a flow chart for explaining reception operation of the individual control packet by the broadcast wave of the broadcast receiving set shown in drawing 15. Hereafter, based on drawing 15, the flow of processing is explained along with drawing 18.
[0077]First, a packet is passed to the individual control information decoding part 104 from the filter part 116. With reference to the information identifier of the packet concerned, when the packet concerned is an individual control packet for contract information distribution, the same processing as the case (refer to drawing 14) of a 1st embodiment is performed (Step S71 - Step S76).
[0078]In the individual control information decoding part 104, when the packet concerned is a command packet, with reference to the command identifier in a packet, it is confirmed whether the packet concerned is a power turn command packet (Step S77). Processing will be ended if the packet concerned is not a power turn command packet.
[0079]When it is a power turn command packet, receiving set ID of the self-device stored in the receiving set ID storage 106 and every one receiving set ID in the packet concerned are compared (Step S78). Processing is ended when receiving set ID of the self-device is not contained in the packet here. When contained, the packet concerned is sent to the individual control information authentication section 107.
[0080]In the individual control information authentication section 107, verification keys are acquired from the digital signature verification-keys storage 108, and a digital signature is verified (Step S79). End processing, when verification of a digital signature goes wrong, and when it succeeds, the signal of the purport (a power turn is used) that the electric power supply to the function part concerning the two-way communication function of the modem section 101 and transmission and reception section 102 grade is started is sent to the power-supply-management department 125, In response to it, the power-supply-management department 125 starts supply of the electric power to these function parts, and changes it into the state waiting for mail arrival always (Step S80).
[0081]Since a two-way communication function will be in the state waiting for mail arrival at

Step S80, the broadcast receiving set can receive the individual control packet for contract information distribution via a two-way communication circuit in a procedure as shown in drawing 9 after that.
[0082]Although the power supply said here means the standby power supply (electric power) for the waiting for the arrival of a two-way communication circuit, depending on composition, the power turn (or OFF) of other formation parts becomes possible by the command packet concerned. Even if the power-supply-management department 125 does not receive the power supply turned on by this embodiment after receiving the individual control packet for contract information distribution via a two-way communication circuit or, it is desirable to turn off after fixed time.
[0083]Thus, by dividing an individual control packet into a broadcast wave and communication, and transmitting, an effective conditional access system can consist of meanings of zone reduction and power saving. Explanation of the 1st variation is finished above.
[0084](A 3rd embodiment) The 2nd variation of a 1st embodiment is explained. In order to transmit individual control information using a two-way communication circuit from a center, it is a variation about the method which performs call origination from the broadcast receiving set side. Since call origination is not uniformly distributed if call origination is performed from the receiving set side, it may be unreceivable by the center side system. This embodiment tends to solve this problem. In this embodiment, a means by which the receiving set which is carrying out call origination attests whether it is a just thing is formed. Although attestation is not necessarily required for the purpose of making call origination uniform, if unlike the 1st - center call origination like a 2nd embodiment the justification of a receiving set cannot attest easily in the case of receiving set call origination and it does not have an authentication means, it will be hard to maintain safety.
[0085]The composition of the important section of the broadcast receiving set concerning a 3rd embodiment is shown in drawing 19. In drawing 19, it differs from the case where the processing operation which receives the individual control packet distributed by a broadcast wave is a 1st embodiment. Therefore, below, only the composition and reception operation of the individual control packet which receives from a broadcast wave are stopped to explain.
[0086]In a 3rd embodiment, the individual control packet received by a broadcast wave is two kinds, the object for contract information distribution, and the object for command distribution (command packet), like a 2nd embodiment. Although the data configuration of the individual control packet for contract information distribution is the same as that of what was explained by a 1st embodiment (refer to drawing 7 (b)) and the composition of a command packet is the same as that of what was explained by a 2nd embodiment (refer to drawing 16 and drawing 17), According to this embodiment, the points that a command identifier directs the call origination to a center to a broadcast receiving set and of being an identifier of a command differ. Hereafter, such a command is called a call origination command and the packet is called a call origination command packet.
[0087]Drawing 20 is a flow chart for explaining reception operation of the individual control packet by the broadcast wave of the broadcast receiving set of drawing 19, and, below, explains the flow of processing along with drawing 20 based on drawing 19.
[0088]First, the individual control packet received by the broadcast wave is passed to the individual control information decoding part 104 from the filter part 116. With reference to the information identifier of the packet concerned, the packet concerned performs the same processing (refer to drawing 14) as a 1st embodiment, when it is a packet for contract information distribution (Step S91 - Step S96).

[0089]When the packet concerned is a command packet, with reference to the command identifier in a packet, it is confirmed whether the packet concerned is a call origination command packet (Step S97). Processing will be ended if the packet concerned is not a call origination command packet.
[0090]When it is a call origination command packet, receiving set ID of the self-device stored in the receiving set ID storage 106 and every one receiving set ID in the packet concerned are compared (Step S98). Processing is ended when receiving set ID of the self-device is not contained in the packet here. When contained, the packet concerned is sent to the individual control information authentication section 107.
[0091]In the individual control information authentication section 107, verification keys are acquired from the digital signature verification-keys storage 108, and a digital signature is attested (Step S99). When verification of a digital signature goes wrong, processing is ended, when it succeeds, the signal of the purport that the call origination to a center is directed in the center call origination part 162 is sent, and the center call origination part 162 performs call origination to a center through the communications department 152 between centers, and the modem section 101 (Step S100).
[0092]Thus, in the conditional access system which transmits an individual control packet using both a broadcast wave and two-way communication, By pointing to the call origination from a receiving set from the center side, making it perform, and managing the generating timing of call origination by the center side, when connecting the two-way communication circuit between centers with the receiving set concerned by the call origination from the receiving set side, For example, the situation where a circuit is not connected easily and becomes a center is avoidable by concentrating on a time zone with the call origination from a receiving set.
[0093]Next, processing operation is explained after a broadcast receiving set performs call origination to a center until it receives an individual control packet. The packet transmitted and received by the two-way communication between a center and a broadcast receiving set consists of an information identifier and an information body, as shown in drawing 21. It can classify into three packets according to the difference in this information body. Here, there are an individual control packet shown in drawing 7 (a), same packet (hereafter, in order to distinguish two kinds of other packets, it is dared to call this packet an individual control packet), a challenge packet, and a response packet, for example.
[0094]The individual control packet consists of an information identifier, a master key identifier, and enciphered contract information, as shown in drawing 22. Contract information is the same as that of drawing 5 here. It consists of an information identifier, and the challenge number and challenge information body for identifying that a challenge packet is a challenge packet as shown in drawing 23, and a challenge number is the question from a center to a receiving set and the management number in question which are called a challenge. The challenges currently assumed by this embodiment are the challenge which asks receiving set ID, the challenge which asks a master key identifier, and a challenge which creates a signature with a secret key (it is peculiar to each receiving set) to challenge information. In addition, the challenge etc. which make the enciphered challenge information decode with a secret key and to which the response of the decoding result is carried out are considered. Like the challenge made to sign with a secret key here, when object data is required, it is described to a challenge information body and it transmits.
[0095]It is in asking a question that it cannot be answered that the foundations of a challenge and response do not use the information which cannot know only a broadcast receiving set and a center, and checking that it is were able to reply to the question correctly, and the broadcast

receiving set concerned is a just (it registers with the center) device.
[0096]It is an information identifier for identifying that a response packet is a response packet as shown in drawing 24 from the challenge number, the challenge information body, and the response information body. Suppose that form has also become the response information body settled by the challenge number (to a challenge information body and the appearance).
[0097]Drawing 25 is the flow chart which showed the processing operation after a receiving set receives a call origination command, and explains the flow of processing along with drawing 25 hereafter based on drawing 19. First, if call origination is performed from a receiving set to a center (Step S101) and a two-way communication circuit is connected with a receiving set between centers, an individual control packet will be transmitted from a center. The center communication analyzing parts 151 of a receiving set receive an individual control packet via the connected two-way communication circuit concerned, the modem section 101, and the communications department 152 between centers (Step S102). The packet which received is passed to the center communication analyzing parts 151, and discriminates here of which classification it is a packet from the information identifier of the packet.
[0098]The center communication analyzing parts 151 pass it to the response preparing part 152, when the packet concerned which received is a challenge packet (Step S103) (Step S106). When it is an individual control packet for contract information distribution, (Step S104) and the individual control information decoding part 104 are passed (Step S107), and the same processing (Step S3 of drawing 9 - step S9) as a 1st embodiment performs attestation and the storing process of contract information (Step S108). the packet which received -- the above -- when it is not any, either, it transmits to a center via a two-way communication circuit as an error (Step S105).
[0099]Next, creation and transmitting processing operation of a response packet are explained along with the flow chart shown in drawing 26. The response preparing part 152 checks the classification of a challenge with reference to the challenge number in a challenge packet. When it is the challenge which receiving set ID asks, (Step S111), Receiving set ID is taken out from the receiving set ID storage 106 (Step S115), a response packet as changed receiving set ID into the response information form defined beforehand and shown in drawing 23 is created (Step S116), and it transmits to a center (Step S117). When it is the challenge which asks a master key identifier (Step S112), a master key identifier is acquired from the master storage 103, a response packet is created like the above-mentioned, and it transmits to a center (Step S118 - Step S120).
[0100]It acquires out of the packet which received (Step S113) and the challenge information body which is data which should sign when it was the challenge of signature creation (Step S121), A secret key is acquired from the secret key storing part 153, and the signature to a challenge (Step S122) information body is created (Step S123). The created signature is changed into the form of a response information body according to the form defined beforehand, and is transmitted to a center in the form of a response packet as shown in drawing 24 (Step S124 - Step S125). When the transmitted challenge information is not applied to which [the three above-mentioned kinds of], an error is transmitted to a center (Step S114).
[0101]After the center side checks the justification of the receiving set concerned by the above processing from the response packet which received, the individual control packet can be transmitted. In (a 1st embodiment described) and this embodiment, it can be said that the receiving set recognizes the information distributing device (center) side by the digital signature given to the individual control packet. For this reason, it is also possible to think that mutual recognition is performed by this embodiment between a receiving set and a center. However, as a 1st embodiment also described, such a gestalt is not indispensable in this invention, and is

essential. [of the embodiment the center side recognizes a receiving set to be like this invention]
[0102]Explanation of the 2nd variation is finished above.
[0103]In the conditional access system which can perform call origination for the individual control packet transmission by two-way communication by a receiving set and center Aikata, a restricted reception system which fills a 2nd and 3rd embodiment simultaneously is also feasible. Since both variations only differ in the kind (command identifier) of command (from the composition) and have a mutually-independent relation, it is both because it is possible to carry out simultaneously. In this meaning, a 1st and 2nd embodiment is broadcast about the command packet according to each receiving set individual, and can realize the individual control packet for contract information distribution to be an embodiment which transmits by two-way communication.
[0104]Although main processings are performed only in the limited reception part 100 in an above embodiment, there is also a view of mounting only the descrambling part 120 on the outside of a limited reception chip. The descrambling part 120 needs high speed processing, in order to have to decode in real time (since broadcast contents are decoded). However, since the other portions must not always operate and processing time moreover has some margins, when it does in this way on mounting, there are many advantageous things. When attaining communalization of a receiving set with other broadcasts, the scrambling system of broadcast contents is held in common by all the broadcasts, and the mounting method which mounts only the limited reception (I would like to hold confidential information by each broadcast) part 100 on the media in which desorption, such as an IC card, is possible can be considered. In the embodiment described above and the embodiment to be described from now on, it is added that the above mounting is also possible.
[0105](A 4th embodiment) A 4th embodiment is a case of the conditional access system which has a master key with all the common broadcast receiving sets. Since the master key is common to all the broadcast receiving sets and the master key (it is common to all the receiving sets) has played the role of the work key in a 1st embodiment, the conditional access system in a 4th embodiment has easy key composition in which a work key does not exist, as shown in drawing 28. Since such a conditional access system has simple composition, it is very useful in respect of transmission amount reduction of individual control information (refer to JP,11-243536,A). (when premised on transmission by a broadcast wave) However, since the master key is common and the channel key of all the channels will be received equally to every broadcast receiving set, in order to realize limited reception, it will be dependent only on channel contract information.
[0106]The composition of the important section of the broadcast receiving set concerning a 4th embodiment is shown in drawing 27. In a 4th embodiment, an individual control packet as shown in drawing 7 is used like the case of a 1st embodiment. However, since a work key does not exist in a 4th embodiment, contract information has the composition which consists of receiving set ID and channel contract information as shown in drawing 29, and a digital signature. As for a common control packet, two kinds, the common control packet for master key creation information distribution (refer to drawing 30 (a)) and the common control packet for channel key distribution (refer to drawing 30 (b)), are used.
[0107]The common control packet for channel key distribution is the same as that of the case (refer to drawing 8) of a 1st embodiment. The common control packet for master key creation information distribution consists of an information identifier, a master key identifier, master key creation information, and a digital signature, as shown in drawing 30 (a).
[0108]Here, an information identifier is the information which shows that the packet concerned is a common control packet for master key creation information distribution, and it is used in order

to distinguish from other packets. A master key identifier is an identifier of the master key generated from the continuing master key creation information. A digital signature is for preventing forgery of the master key creation information concerned, has what is depended on a secret key cryptosystem like the digital signature used by a 1st embodiment, and a thing to depend on public key encryption, and may use whichever.

[0109]Next, the composition and processing operation of the broadcast receiving set of drawing 27 are explained. Since the processing operation of the broadcast receiving set concerning a 4th embodiment has many portions which lap with it of a 1st embodiment, it stops to explain only a different portion.

[0110]drawing 31 is explained with reference to the flow chart boiled and shown about reception operation of a common control packet. In drawing 31, a receiving set receives a common control packet, and when a common control packet is passed to the common-control-information decoding part 117 from the filter part 116, it is started.

[0111]First, the common-control-information decoding part 117 judges whether the packet concerned is for channel key distribution with reference to the information identifier of the receive packet concerned (Step S301). If it is a common control packet for channel key distribution, a master key identifier will be extracted from the non-code portion of the packet concerned, and the master key which has the master key identifier concerned will be acquired from the master key storing part 105 (Step S302). The encryption section of a packet is decoded using the acquired master key (Step S303). The channel key obtained as a result of decoding is stored in the channel key storage 118, and it ends.

[0112]On the other hand, if the packet which received is a common control packet for master key creation information distribution (Step S305), A master key identifier is taken out from the packet concerned, and it is judged whether the master key corresponding to the master key identifier exists in the master key storing part 103 (Step S306). When it already exists, it ends there. When it does not exist, a master key new next is generated.

[0113]First, the master key creation information verification part 181 is the master key generation part 182, when the verification failure of the digital signature contained in the packet concerned is verified and (Step S307) carried out and a verification success is ended and carried out, A master key is generated according to the algorithm beforehand defined from the master key creation information included in the packet concerned (Step S308), and the generated master key is stored in the master key storing part 103, and it ends (Step S309).

[0114]Here, a little explanation of master key creation information and master key generation processing must be given. Master key creation information is the random number seed information for for example, master key generation, and the means of the random number generation with the algorithm and parameter of random number seed and the master key generation part 182 which were defined beforehand generates a master key. Since generation is performed in the Tampa-proof hardware, the problem of safe does not have master key creation information with un-enciphering.

[0115]Operation is the same as that of a 1st embodiment than reception of the individual control packet transmitted by two-way communication.

[0116]It is possible to apply the variation (a 2nd and 3rd embodiment) of a 1st embodiment also to a 4th embodiment.

[0117](A 5th embodiment) A 5th embodiment explains the information distributing device (it is also called a contract-management center device or a contract-management device) formed in the center side for distributing an individual control packet common control packet to the broadcast receiving set concerning a 1st embodiment.

[0118]Drawing 32 is what showed the example of composition of the important section of the information distributing device concerning a 5th embodiment, and it explains hereafter the composition and processing operation of an information distributing device which are shown in drawing 32 along with the flow chart shown in drawing 35 - drawing 39, referring to drawing 32.
[0119]All the members' subscriber data is stored in the subscriber database (DB) 202 in drawing 32. As the data configuration of a subscriber data is shown in drawing 33, it consists of member ID, receiving set ID, a master key identifier, a master key, channel contract information, the transmitted flag, a broadcast transmission flag, and a call number, and this is a subscriber data of one affair.
[0120]Member ID is the management number added to each member, and in this embodiment, since it is easy, it is assumed that it waves from No. 1 to "MAXID" watch. Receiving set ID shows receiving set ID of the member who shows member ID. A master key identifier is an identifier of the master key which exists in the inside of the receiving set of the member concerned (master key storing part 103) now, and a master key is a master key corresponding to the master key identifier concerned. Channel contract information expresses the contract condition of the member concerned, as shown in drawing 2 and drawing 6. A transmitted flag is a flag which shows the member concerned whether the channel contract information concerned was transmitted in two-way communication, and it becomes finishing at the time of "0" transmitting at un-transmitting and the time of "1." It is a flag which shows whether the broadcast transmission flag should carry out broadcast distribution of the channel contract information concerned of the subscriber data concerned, and it is shown at the time of "0" that it is not necessary to carry out broadcast distribution, and it is shown at the time of "1". [it] [necessary] [to carry out broadcast distribution]
[0121]Here, distribution of an individual control packet shall be first distributed in two-way communication. In that there was no response as which ******** and the error which did not carry out normal reception have been answered also for having tried call origination repeatedly to the receiving set which should receive it etc., in that case, distribution of the individual control packet shall be changed at broadcast distribution. The number of times of the call origination which will be permitted by the time it changes distribution of the individual control packet to a broadcast receiving set from two-way communication to broadcast distribution is set to N. A call number presupposes that it is a telephone number of the two-way communication circuit connected to the receiving set of the member concerned.
[0122]First, the processing operation at the time of transmitting the individual control packet in the information distributing device of drawing 32 in two-way communication is explained along with the flow chart shown in drawing 35. This processing is periodically started by the individual control information control part 206 at every renewal of a work key.
[0123]The individual control information preparing part 203 which received individual control packet creation directions from the individual control information control part 206, It is referred to as the variable k= 0 (Step S3301a) and i= 1 (Step S301b), and it is confirmed whether the subscriber data whose member ID is i exists in the member DB202 (Step S302). The processing at the time of not existing is described. When it does not exist, it progresses to Step S313 and one i is **********ed, and after checking that i does not exceed "MAXID", it returns to (Step S314) and Step S302, and member ID is checked by new i.
[0124]Since it means that general processing was completed about all the subscriber datas at Step S314 if i exceeds "MAXID", Next, it is inspected whether it progresses to Step S315, member DB202 is all searched, and an untransmitted subscriber data exists (is there any subscriber data whose transmitted flag is "0" or not?). If there is an untransmitted subscriber data here, one k

(meaning of the k-th search of the subscriber data in the member DB302) will be **********ed (Step S316), When k exceeds N (maximum of the number of times of call origination) (Step S317), the transmitted flag of a subscriber data at the time about the member of "0." It gives up distributing an individual control packet by two-way communication, and a transmitted flag sets the broadcast transmission flag of the subscriber data of all the members of "0" to "1", and is completed (Step S318). If k does not exceed 1, it returns to Step S301b, and processing is repeated after using i= 1. In Step S315, if a non-transmission flag does not have a member record of "0", it will end. When k does not exceed N, i= 1 is used and this algorithm is performed from the beginning. It will end, if there is no untransmitted subscriber data.

[0125]At Step S302, when the subscriber data of i exists, since it is ending with transmitting if member ID is "1", with reference to the transmitted flag in the subscriber data concerned, If i is not over "MAXID" after progressing to Step S313 and **********ing one i (Step S314), it returns to Step S302 and returns to a member ID's existence check. Since the processing which performs a member ID's existence check while carrying out 1 ** increment of the i until it exceeds this "MAXID" is processing which appears frequently even in the bottom, since it is easy, it is carried out to calling it increment processing by the following explanation.

[0126]At Step S302, when the subscriber data of member ID=i exists, since it is ending with transmitting if it is "1", one i is **********ed and it returns to a member ID's existence check with reference to the transmitted flag of the subscriber data concerned. When a transmitted flag is "0", the individual control information preparing part 203 acquires a required work key from work key DB210 based on the channel contract information of the subscriber data concerned (Step S304). Since it assumes that the work key is set up for every channel (a 1st embodiment also explained like), the processing which acquires the work key only for the channel only a contract of was made in this way is needed here.

[0127]Receiving set ID of the work key with which the individual control information preparing part 203 was acquired, and the subscriber data concerned, Using the digital signature generation key which creates contract information main parts other than a digital signature from channel contract information, and is stored in the digital signature generation key storing part 205, this contract information main part. Or a digital signature is created by enciphering a contract information main part and the hash value as the characteristic quantity, and contract information as shown in drawing 5 is created. This created contract information is enciphered with the master key in the subscriber data concerned, a master key identifier and an information identifier are added, and an individual control packet as shown in drawing 7 (a) is created (Step S305).

[0128]The created packet is passed to the transmitting and receiving controller 207 with the call number in the subscriber data concerned via the individual control information control part 206, and the transmitting and receiving controller 207 carries out call origination of the broadcast receiving set shown in drawing 1 of the member concerned using this call number (Step S306). When the receiving set concerned does not return a response to this call origination, a receiving error is outputted from (Step S307) and the error output part 215 (Step S308), and it progresses to Step S313, increment processing is performed, and processing is moved to the following subscriber data.

[0129]In Step S307, when the response has returned from the receiving set concerned to call origination, the created individual control packet is transmitted with the protocol defined beforehand (Step S307). When fixed time has acknowledgment of receipt from a receiving set after transmission (Step S310), the individual control information control part 206, The transmitted flag of the subscriber data concerned is set to "1" (Step S312), and after progressing to Step S313 and performing increment processing, processing is moved to the following

subscriber data.
[0130]As the portion of increment processing also described, i exceeds "MAXID", it checks that all the subscriber datas are ending with transmitting, or (Step S315) k exceeds the default N, and this processing ends it, when distribution by the two-way communication of an individual control packet is given up (Step S318).
[0131]Next, the formation part concerning the transmitting processing operation and this transmitting processing operation for transmitting a common control packet and an individual control packet by broadcast of drawing 32 is explained along with the flow chart shown in drawing 36. It is started simultaneously with a broadcast start, and this processing is repeated without an intermission, while broadcast continues. First, the common-control-information preparing part 209 searches the channel key database (DB) 211, and acquires channel key data with the minimum channel ID (Step S401).
[0132]Channel key data is data for every channel registered into channel key DB211 which contains a channel key at least, and is having here structure shown in drawing 34. Channel key data consists of channel ID, a channel identifier, the channel key identifier (1), the channel key (1), a channel key identifier (2), and a channel key (2). Channel ID is a number on DB management wave to each channel here. The channel identifier is the same as it which was explained by the 1st - a 4th embodiment for information for a broadcast receiving set to identify each channel. A channel key identifier and a channel key are the same as what was described by the 1st - a 4th embodiment.
[0133]it is because that 2 sets of pairs of a channel key and its identifier exist here needs to transmit now an effective channel key (channel key (1)) and the channel key (channel key (2)) used for the next together, and is used now depending on composition -- only a channel key is not cared about.
[0134]First, the creation command of a common control packet is made from the broadcast transmission control part 213 to the common control information control part 212. It is directed that the common control information control part 221 searches channel key DB211 to the common-control-information preparing part 209, and searches channel key data with the minimum channel key ID with this command. In response, the common-control-information preparing part 209 searches channel key DB211, and acquires channel key data (Step S401).
[0135]The creation command of an individual control packet is made from the broadcast transmission control part 213 to the individual control information control part 206. With this command, the individual control information control part 206 searches member DB202 to the individual control information preparing part 203, and directs to search the subscriber data in which a broadcast transmission flag has the minimum member ID that is "1." In response, the individual control information preparing part 206 searches member DB202, and acquires a subscriber data (Step S406).
[0136]On the other hand, in the common-control-information preparing part 209, a channel identifier, a channel key identifier (1), a channel key (1), a channel key identifier (2), and a channel key (2) are acquired from the acquired channel key data, and a common control packet as shown in drawing 8 is created (Step S404). In that case, a channel identifier is used as a key, work key DB210 is searched, the effective work key to the channel concerned is extracted, and the portion as which a common control packet should be enciphered using the work key concerned is enciphered. The work key identifier and information identifier of the work key concerned are attached, a common control packet is generated, and it sends to the broadcast transmission section 214 via the common control information control part 212 and the broadcast transmission control part 213, and the packet concerned is put on a broadcast wave and sent in

the broadcast transmission section 214 (Step S405).
[0137]Next, in the individual control information preparing part 206, channel contract information is extracted from the acquired subscriber data, and a required work key is acquired from work key DB204 based on this (Step S407). Like the case where it distributes by two-way communication, contract information main parts other than a digital signature are created from receiving set ID in a work key and the subscriber data concerned, and channel contract information, and contract information is created using the digital signature generation key stored in the digital signature generation key storing part 205. Contract information is enciphered with the master key in the subscriber data concerned, a master key identifier and an information identifier are added, and an individual control packet is created (Step S408). Via the individual control information control part 206, the created packet is passed to the broadcast transmission control part 213, from here, puts the packet concerned on a broadcast wave, and sends it (Step S409).
[0138]The above-mentioned processing operation shows the example which carries out broadcast transmission of a common control packet (common control packet for channel key distribution), and the individual control packet (individual control packet for contract information distribution) by turns. However, if how many this former is distributed, originally the distribution rate how many the latters to distribute is decided at convenience [of a broadcasting organization], and change of a rate can be realized easily.
[0139]It returns to explanation of drawing 36 and generation of the following transmitting packet is started, respectively in the stage which transmission of 1 set of common control packets and an individual control packet ended. That is, in the common control information control part 212, the directions from the broadcast transmission control 213 extract the following channel key data from channel key DB211 (Step S410). The following channel key data is channel key data which has large channel ID in the next of channel ID of the channel key data concerning the common control packet which transmitted previously here. When there is no such channel key data here, channel key data with the minimum channel ID is extracted from channel key DB211 (Step S414).
[0140]The minimum thing in inside [that the broadcast transmission flag exceeded similarly member ID of the subscriber data whose member ID has processed / said / among the subscriber datas which are "1" about the subscriber data] is extracted (Step S412). Here, if there is no such subscriber data, a subscriber data with the minimum member ID will be extracted (Step S402).
[0141]The these-extracted data performs packet creation / transmitting processing which was mentioned above in the common-control-information preparing part 212 and the individual control information preparing part 203, respectively. Thus, it continues moving without an intermission from a broadcast start.
[0142]Generation of a common control packet and generation of an individual control packet can be performed in parallel so that clearly also from the above explanation. This is because generation/transmission of two kinds of packets can be controlled by the broadcast transmission control part 213 and it can transmit at a fixed rate.
[0143](A 6th embodiment), next some variations are described. As the 1st variation, a power turn command from a center to the broadcast receiving set concerning a 2nd embodiment of distributing to each receiving set individually A command packet, The information distributing device (it is also called a contract-management center device or a contract-management device) formed in the center side for distributing an individual control packet and a common control packet is explained. This 1st variation is explained as a 6th embodiment.
[0144]As the 2nd variation, a call origination command is individually distributed to each

receiving set from a center, As opposed to the broadcast receiving set concerning a 3rd embodiment of making a center carry out call origination from the receiving set side, The information distributing device (it is also called a contract-management center device or a contract-management device) formed in the center side for distributing a command packet, an individual control packet, and a common control packet is explained. This 2nd variation is later mentioned as a 7th embodiment.

[0145]Although the example of composition of the important section of the information distributing device concerning a 6th embodiment is the same as the case (drawing 32) of a 5th embodiment, processing operation differs. First, after distributing a power turn command packet in a broadcast wave, the case where individual control information is distributed by two-way communication is explained along with the flow chart shown in drawing 37 - drawing 38.

[0146]This processing is started according to a contract modification stage (every [for example,] month). If a contract modification stage comes, the individual control information control part 206 will be a receiving set which should transmit the contract information for updating channel contract information etc. to the individual control information preparing part 206 first, and will order to still transmit a power turn command one by one to the receiving set which has not transmitted the contract information. The individual control information preparing part 203 receives this, member DB202 is searched, and a transmitted flag takes out a maximum of M subscriber datas of "0" from what has small member ID (Step S501). Here, M is a constant decided by the information capacity and others of a power turn command packet.

[0147]Next, since receiving set ID is extracted from the extracted subscriber data, respectively (Step S502) and a digital signature is attached to the row of the number of extracted receiving set ID and these receiving set ID, A digital signature generation key is extracted from the digital signature generation key storing part 205 (Step S504), the number of receiving set ID and these receiving set ID is enciphered with the key concerned, and a digital signature is generated (Step S505). The command main part of a data format as shown in drawing 17 from the number of extracted receiving set ID and these receiving set ID, a digital signature, and the command identifier of a power turn command is created. Thus, an information identifier is attached to the made command main part, and a command packet is generated (Step S506). The generated command packet is sent to the broadcast transmission section 214 via the individual control information control part 206 (Step S507), and is stored in the buffer memory in the broadcast transmission section 214 temporarily, and broadcast transmission is carried out with a common control packet in the procedure mentioned later (refer to drawing 39).

[0148]Next, processing which distributes the individual control packet for it to the broadcast receiving set which must update channel contract information etc. is performed. Based on the channel contract information in the i-th subscriber data, a work key is extracted from work key DB210 among M (maximum) subscriber datas extracted at (Step S508) and Step S501 as i= 1 (Step S509). An individual control packet (individual control packet for contract information distribution) is created still like explanation of a 5th embodiment (Step S510). Next, call origination is carried out using the call number in the subscriber data concerned (Step S511), and the broadcast receiving set and two-way communication of the call origination point are started. When the receiving set concerned to a response cannot be found here, the error of the purport of (Step S512) and a receiving error is returned to the individual control information control 206, In individual control ********** 206, this is displayed in the error output part 215 (Step S522), it progresses to Step S516 of drawing 38, and processing is moved to the following subscriber data.

[0149]At Step S512, when the response has returned from the broadcast receiving set of the call origination point, the created individual control packet is transmitted (Step S513). By the time it

goes through the predetermined time defined beforehand after individual control packet transmission, From the receiving set concerned, when there is no acknowledgment of receipt, return the error of the purport of (Step S514) and a receipt error to the individual control information control part 206, and in the individual control information control part 206. The purport of a receipt error is displayed on the error output part 215, it progresses to Step S516 of drawing 38, and processing is moved to the following subscriber data.

[0150]When there is acknowledgment of receipt at Step S514, it progresses to Step S515 of drawing 38, and the transmitted flag of the i-th subscriber data concerned is set to "1", it progresses to Step S516, and processing is moved to the following subscriber data.

[0151]The following processings are required when moving processing to the following subscriber data. That is, it is confirmed whether (Step S516) and i exceed M as i=i+1 (Step S517). If the i-th subscriber data exists when not exceeding (Step S518), it will return to Step S509 and will process to the subscriber data like the above-mentioned henceforth. When a subscriber data does not exist, it progresses to Step S519, member DB202 is searched with Step S518, and a transmitted flag extracts M (maximum) records next to "0" at it (Step S519). If one or more subscriber datas can be extracted here (Step S520), it will return to Step S502 and the power turn command over the subscriber data group will be created. At Step S520, since it means that round processing was completed when a subscriber data is not extracted, member DB202 to one checks whether all the subscriber datas of member DB202 are searched, and a transmitted flag has a thing of "0" (Step S521). If it is here, it returns to Step S501 and is the same as that of the above-mentioned henceforth. At Step S521, if the thing of "0" does not have a transmitted flag, since it is ending with transmitting, it will end about all the subscriber datas.

[0152]On the other hand, at Step S517, when i exceeds M, Since the individual control packet to the receiving set which carried out broadcast transmission of the power turn command will finish transmitting, it progresses to Step S519, member DB202 is searched, and a transmitted flag extracts the following M (maximum) subscriber datas that are "0." If one or more subscriber datas can be extracted here (Step S520), it will return to the place (Step S502) which creates a power turn command to the subscriber data group, and will repeat. Since it means that round processing had ended one at Step S520 when a subscriber data is not extracted, it is checked whether all the subscriber datas of member DB202 are searched, and a transmitted flag has a thing of "0" (Step S521). If at least one subscriber data is extracted here, it will return to the beginning of processing of Step S501. If a subscriber data is not extracted, since one is ending with transmitting, it is ended about all the subscriber datas.

[0153]After the above carries out broadcast distribution of the power turn command, it is processing operation until it transmits an individual control packet in two-way communication. As opposed to the broadcast receiving set of composition as the individual control packet was shown in drawing 1 which transmits in two-way communication after this according to this embodiment, Since call origination for individual control packet distribution is performed from the center side (information distributing device of drawing 32) after issuing the directions which make one the power supply of the formation part which starts two-way communication via a broadcast wave beforehand and changing the ********** concerned into the state waiting for mail arrival, To the broadcast receiving set which can receive an individual control packet, an individual control packet can be certainly distributed by two-way communication in two-way communication.

[0154]Next, the transmitting processing operation of the transmit information of a common control packet is explained along with the flow chart shown in drawing 39. It is started at the time of a broadcast start, and this processing is continued without an intermission henceforth till the

end of broadcast.
[0155]First, it directs to search the channel key data which has the minimum channel key ID from the common control information control part 212 to the common-control-information preparing part 209 (Step S601). Channel key DB211 is searched with the common-control-information preparing part 209 in response to these directions, and a channel key is acquired. A channel identifier, a channel key identifier (1), a channel key (1), a channel key identifier (2), and a channel key (2) are acquired from the acquired channel key data, and a common control packet as shown in drawing 8 is created (Step S602). In that case, a channel identifier is used as a key, work key DB210 is searched, the effective work key to the channel concerned is extracted, and the portion as which a common control packet should be enciphered using the work key concerned is enciphered. The work key identifier and information identifier of the work key concerned are attached, a common control packet is generated, and it sends to the broadcast transmission section 214 via the common control information control part 212 and the broadcast transmission control part 213, and the packet concerned is put on a broadcast wave and sent in the broadcast transmission section 214 (Step S603).
[0156]Next, the broadcast transmission section 214 confirms whether the power turn command packet created by processing of Step S501 of drawing 37 - Step S507 exists in the buffer memory (Step S604), The time of being created among the command packets concerned, when it exists carries out broadcast transmission of the oldest thing from the broadcast transmission section 214 (Step S605), and it progresses to Step S606, and on the other hand, when it does not exist, Step S605 is skipped and it progresses to Step S606.
[0157]The command of the purport that the channel key data of following channel key ID is searched with Step S606 from channel key DB211 is transmitted to the common-control-information preparing part 209 via the common control information control part 212 from the broadcast transmission control part 213, Channel key DB211 is searched with the common-control-information preparing part 209, and channel key data is extracted (Step S606). When it succeeds in extraction, creation/transmitting processing of the common control packet for the channel key distribution concerned after (Step S607) and Step S602 is performed here, When extraction has gone wrong, it returns to the processing beginning of Step S601, and the channel key data which has the minimum channel key ID again is searched.
[0158]Thus, by transmitting the common control packet for channel key distribution for 1 or two or more power turn command packets (if it generally says command packet), 1 or when distributing more than one, It cannot interfere with transmission of the common control packet for channel key distribution, but a command packet can be transmitted timely.
[0159]The frequency issues of a power turn command are considered that 1 time cannot be found in 1 second, either from the air time of an individual control packet, etc. to the channel key usually (for a timely receiving start) having to transmit twice in 1 second. For this reason, the rate of the number of power turn command packets which it has at the time of common control packet distribution and which should be distributed is very low. Since being transmitted immediately is expectable after a power turn command packet is created from this and it is sent to the broadcast transmission control part 213, When carrying out call origination of the broadcast receiving set for individual control packet transmission, it may be thought that the power supply of the two-way communication circuit by the side of a receiving set is already turned on.
[0160](A 7th embodiment) A call origination command is individually distributed to each receiving set from a center, As opposed to the broadcast receiving set concerning a 3rd embodiment of making a center carry out call origination from the receiving set side, The information distributing device (it is also called a contract-management center device or a

contract-management device) formed in the center side for distributing a command packet, an individual control packet, and a common control packet is explained.
[0161]The example of composition of the important section of the information distributing device concerning a 7th embodiment is shown in drawing 40, and the creation processing operation of a command packet is explained along with the flow chart shown in drawing 41, referring to drawing 40. This processing operation is started for every month according to alteration time, such as channel contract information. The individual control information control part 206 will order to transmit a call origination command to the individual control information preparing part 203 one by one to the receiving set of renewal of un-[channel contract information] first, if alteration time, such as channel contract information, comes. 203 receives this, member DB204 is searched with an individual control information preparing part, and a transmitted flag takes out a maximum of M subscriber datas of "0" from what has small member ID (Step S611). Since a digital signature is attached to the row of the number of extracted receiving set ID and these receiving set ID, A digital signature generation key is extracted from the digital signature generation key storing part 205 (Step S612), the number of receiving set ID and these receiving set ID or the hash value as these data rows and its characteristic quantity is enciphered with the key concerned, and a digital signature is generated (Step S613). The command main part of a data format as shown in drawing 17 from the number of extracted receiving set ID and these receiving set ID, a digital signature, and the command identifier of a call origination command is created. Thus, an information identifier is attached to the made command main part, and a call origination command packet is generated (Step S614).
[0162]The generated call origination command packet is sent to the individual broadcast transmission control part 213 via the individual control information control part 206 (Step S615), and as shown below, broadcast transmission is carried out with other common control packets.
[0163]The transmitting processing operation of the individual control packet by two-way communication is explained according to the flow chart shown in drawing 42 - drawing 43, referring to drawing 40. This processing is started by the call origination from a broadcast receiving set (Step S701). In the center, call origination is received from a receiving set by the transmitting and receiving controller 207 via the modem 208 (Step S702), and a creation command of the challenge which asks receiving set ID is sent to the challenge preparing part 252 in the transmitting and receiving controller 207. In the challenge preparing part 252, the challenge packet of composition of having been shown in drawing 23 which asks receiving set ID in response is created. The challenge database (DB) 251 is a database with which the challenge number of various challenges and the group of processing were indicated here. The challenge preparing part 252 uses as a key the challenge number which asks challenge DB251 to receiving set ID, and extracts the contents of processing. The created challenge packet is transmitted to a receiving set via the modem 208 from the transmission and reception section 207 (Step S703). When a response packet is not transmitted from the receiving set concerned into the predetermined time beforehand defined after transmission (Step S704), the individual control information control part 206, The error output of the purport of challenge failure that receiving set ID is asked is outputted from the error output part 215, and the processing to the receiving set concerned is ended (Step S717).
[0164]When the response packet has been transmitted into predetermined time at Step S704, the response packet is sent to the response verification part 253 from the transmitting and receiving controller 207. In the response verification part 253, after conducting the format check of the response packet concerned, receiving set ID taken out from the packet is outputted to the transmitting and receiving controller 207 (Step S705). the transmitting and receiving controller

207 extracts the subscriber data of the receiving set ID concerned from member DB202 for this receiving set ID to the individual control information control part 206 to a key -- a purport command is carried out. Here, since the receiving set ID concerned does not exist without an applicable subscriber data (Step S705), an error output etc. are performed and processing is ended (Step S722). If a subscriber data is acquired (Step S706), the subscriber data concerned will be sent to the transmitting and receiving controller 207, and the transmitting and receiving controller 207 will send it to the response inspection section 253.

[0165]Then, like the case of the challenge creation as which the transmitting and receiving controller 207 inquires receiving set ID to the challenge preparing part 252, It points to the challenge creation which asks a master key identifier, the challenge packet created as a result is transmitted (Step S707), and the response packet sent in predetermined time is inspected (Step S708, Step S709). When the master key identifier is not in agreement with it of the subscriber data concerned, the error output of the purport of master key identifier disagreement is performed (Step S719), and when in agreement, it shifts to processing of receiving set attestation in which it explains below.

[0166]Receiving set authenticating processing is processing which generates one or more challenges made to answer using the information known only with a just receiving set, and attests by the response. First, by the transmitting and receiving controller 207, it is set as j= 1 (Step S710), and it is requested that an attestation challenge should be published to the challenge preparing part 252. In the challenge preparing part 252 which received the request, a challenge is extracted from challenge DB251 at random, a challenge packet as shown in drawing 23 is created (Step S711), and it is transmitted to a broadcast receiving set via the modem 208 from the transmitting and receiving controller 207 (Step S712). When a response packet is not sent from a receiving set within after-transmission fixed time (Step S713), the error output of the purport of attestation challenge failure is performed, and it ends (Step S720). When the response packet has been sent, the response packet is sent to the response verification part 253 from the transmitting and receiving controller 207, and conducts an attestation inspection by the authentication algorithm provided in challenge DB251 in the response verification part 253 (Step S714). Since it was shown that it is a right response when an attestation inspection was successful, it is confirmed whether ********** one j (Step S715) and j exceeds N (Step S716). N is the constant for which it depended on the system beforehand, and means the trial frequency of an attestation challenge. When j does not exceed N, the receiving set authenticating processing of Step S711 - Step S714 is repeated until j exceeds N. When an attestation inspection fails in Step S714, since it is the wrong response, the error output of the purport of an authentication failure is performed and it ends (Step S721).

[0167]When j exceeds N at Step S716, it will mean that attestation was completed and it is able to be checked that the receiving set which is performing the present communication by the information distributing device (center) side is just. Then, it progresses to Step S722 of drawing 43, and the signal of the end of attestation is sent to the individual control information control part 206 from the transmitting and receiving controller 207, and the individual control information control part 206 is requested from the individual control information preparing part 203 so that the individual control packet of the subscriber data concerned may be created. In response in the individual control information preparing part 203, a required work key is acquired from work key DB210 based on the channel contract information in the subscriber data concerned (Step S722). Here, since it assumes that the work key is set up for every channel, the processing which acquires the work key only for the channel which is specified in channel contract information, and only a contract of is made is needed.

[0168]Next, contract information main parts other than a digital signature are created from the pair of the work key and work key identifier which were acquired and receiving set ID of the subscriber data concerned, and channel contract information, and contract information is created using a digital signature generation key. Contract information is enciphered with the master key of the subscriber data concerned, a master key identifier and an information identifier are added, and an individual control packet as shown in drawing 22 is created (Step S723). The created packet is sent to the transmitting and receiving controller 207 via the individual control information control part 206, and is transmitted to a receiving set. After the transmission concerned, when fixed time has acknowledgment of receipt from a receiving set, the transmitted flag of the subscriber data concerned (Step S724) is set to "1", and it ends (Step S725). When there is no acknowledgment of receipt, the error output of the purport of receipt failure of an individual control packet is performed, and it ends (Step S726).
[0169]According to a 7th embodiment of the above, so that the call origination from the receiving set side may not concentrate on one time, Even if the stage of the call origination from the receiving set side can be adjusted from the center side and also it is the call origination from the receiving set side, after attesting the justification of a receiving set, Since the individual control packet for updating the channel contract information etc. which are stored in the receiving set can be transmitted, injustice which becomes other receiving sets, and clears up and carries out call origination to them can be prevented.
[0170]Since the 1st variation is premised on receiving set call origination for the 2nd variation on the assumption that center call origination so that clearly also from the above explanation, it is also possible to perform this simultaneously. That is, it constitutes so that an individual control packet may be transmitted by a broadcast wave, when not transmitting and carrying out center call origination of the power turn command packet about the receiving set which does not carry out call origination at all or still not receiving, even if it transmits a call origination command packet. If it does in this way, the transmitter meeting of an individual control packet will increase more, and a trouble by which renewal of a contract is not carried out to that unjust viewing and listening can be prevented and having contracted will also decrease.
[0171]Although based on transmission of the individual control packet by the two-way communication by center call origination, combining these and a 5th embodiment, Change into the state (power turn state) in which receipt is possible the two-way communication function part which carries out broadcast distribution of the power turn command packet, and a receiving set has compulsorily about the receiving set which does not answer, or, Broadcast transmission of the call origination command packet is carried out, call origination is carried out from the receiving set side, and the conditional access system which can distribute the individual control packet for renewal of the channel contract information etc. which are memorized by the receiving set by two or more methods can be built. Especially the thing for which it has more transmitting means of an individual control packet about the receiving set which can carry mobile environment (since a receiving set is not in the always same state) is advantageous.
[0172](An 8th embodiment) An 8th embodiment explains the information distributing device (it is also called a contract-management center device or a contract-management device) formed in the center side for distributing individual control information and common control information to the broadcast receiving set explained by a 4th embodiment.
[0173]An 8th embodiment is stopped to explain only a portion which is different since there are many portions which overlap with the 5th - the 7th embodiment and information distributing device on composition and processing operation. That is, even if an individual control packet has some difference in a data configuration, the handling is the same, therefore the formation part and

processing operation for distributing an individual control packet in two-way communication are the same as that of the case of the 5th - a 7th embodiment. So, below, an individual control packet common control packet is extracted and explained to the formation part which carries out broadcast distribution, and its processing operation.

[0174]Being transmitted from the broadcast transmission section 214 in the 5th - a 7th embodiment, To having been a common control packet for channel key distribution, and an individual control packet for distribution of channel contract information etc., the common control packet for channel key distribution at an 8th embodiment, Three, the common control packet for master key creation information distribution and the individual control packet for channel contract information distribution, are assumed. Follow. In an 8th embodiment, broadcast transmission of the three above-mentioned kinds of packets must be carried out. This point is an intrinsically different point from the 5th - a 7th embodiment.

[0175]The example of composition of the important section of the information distributing device concerning an 8th embodiment is shown in drawing 44, and the processing operation at the time of carrying out broadcast transmission of the three above-mentioned kinds of packets is shown in drawing 45 - drawing 46. Hereafter, it explains along with the flow chart shown in drawing 45 - drawing 46, referring to drawing 44.

[0176]It is started simultaneously with a broadcast start, and this processing is repeated without an intermission, while broadcast continues. First, the common-control-information preparing part 209 searches channel key DB211, and acquires channel key data with the minimum channel ID. Channel key data is having here structure shown in drawing 34 by the data for every channel registered into channel key DB211 which contains a channel key at least. Channel key data consists of channel ID, a channel identifier, the channel key identifier (1), the channel key (1), a channel key identifier (2), and a channel key (2). Channel ID is a number on the database management wave to each channel here. The channel identifier is the same as that of the explanation of an embodiment mentioned above for information for a receiving set to identify each channel. It is the same as that of explanation of the embodiment which also mentioned above the channel key identifier and the channel key. Only the channel key which is because that 2 sets of pairs of a channel key and its identifier exist here needs to transmit now an effective channel key and the channel key used for the next together, and is used now depending on composition.

[0177]First, the creation command of the common control packet for channel key distribution is made from the broadcast transmission control 213 to the common control information control part 212. It is directed that the common control information control part 212 searches channel key DB211 to the common-control-information preparing part 209, and searches channel key data with the minimum channel ID with this command. In response, the common-control-information preparing part 209 searches channel key DB211, and acquires channel key data (Step S801).

[0178]The broadcast transmission control part 213 gives the creation command of an individual control packet to the individual control information control part 206. the subscriber data in which the individual control information control part 206 searches member DB202 to the individual control information preparing part 203 with this command, and a broadcast transmission flag has the minimum member ID that is "1" -- search -- it directs like. In response, the individual control information preparing part 203 searches member DB202, and acquires a subscriber data (Step S802).

[0179]From the channel key data acquired in the common-control-information preparing part 209 to next, a channel identifier. A channel key identifier (1), a channel key (1), a channel key identifier (2), and a channel key (2) are acquired (Step S803), and creation of the common control

packet for channel key distribution as shown in drawing 30 (b) is started. That is, an effective master key is extracted from the master key storing part 261, and the data row which consists of a channel identifier, a channel key identifier (1), a channel key (1), a channel key identifier (2), and a channel key (2) is enciphered using the master key concerned. The master key identifier and information identifier of the master key concerned are attached, and the common control packet for channel key distribution is generated (Step S804). This common control packet is sent to the broadcast transmission section 214 via the common control information control part 212 and the broadcast transmission control part 213, and is carried and sent to a broadcast wave from here (Step S805).

[0180]Next, in the individual control information preparing part 203, receiving set ID and channel contract information are acquired from the acquired subscriber data (Step S806), and contract information other than a digital signature is created from them. Using the digital signature generation key stored in the digital signature generation key storing part 205, the data row from receiving set ID to channel contract information, Or this data row and the hash value as that characteristic quantity are enciphered, a digital signature is created, it is given to the last of the data row from receiving set ID to channel contract information, and contract information as shown in drawing 29 is created. Contract information is enciphered with the master key picked out from the subscriber data concerned, a master key identifier, receiving set ID, and an information identifier are added, and an individual control packet as shown in drawing 7 (b) is created (Step S807, Step S808).

[0181]The created packet is sent to the broadcast transmission section 214 via the individual control information control part 206 and the broadcast transmission control part 213, and is carried and sent to a broadcast wave from here (Step S809).

[0182]Next, the common-control-information preparing part 209 creates the common control packet for master key creation information distribution. First, the identifier (master key identifier) of master key creation information and the master key generated from it is acquired from the master key creation information storage 264, Then, the digital signature to master key creation information is created by acquiring a digital signature generation key from the digital signature generation key storing part 205, and enciphering master key creation information or master key creation information, and the hash value as the characteristic quantity, A digital signature and an information identifier are added and the common control packet for master key creation information distribution of composition of being shown in drawing 30 (a) is created (Step S810 - Step S811).

[0183]This created packet is sent to the broadcast transmission section 214 via the common control information control part 212 and the broadcast transmission control part 213, and is carried and sent to a broadcast wave from here (Step S812).

[0184]The above explanation shows the example which carries out broadcast transmission of the common control packet for channel key distribution, the individual control packet for contract information distribution, and the common control packet for master key creation information distribution one by one. However, originally the rate of ******** of the packet which will transmit the following packet if which transmits which packet is decided at convenience [of a broadcasting organization], and change of a rate is easy.

[0185]It is the stage which 1 set of transmission of the common control packet for channel key distribution, the individual control packet for contract information distribution, and the common control packet for master key creation information distribution ended, and shifts to generation of the packet which should transmit to the next. That is, the common-control-information preparing part 209 searches the following channel key data from channel key DB211 (Step S813). Channel

ID is the minimum thing here among channel key data with channel ID with the following larger channel key data than channel ID of the channel key data concerning the packet which transmitted previously. When there is no such channel key data here, channel key data with (Step S814) and the minimum channel ID is extracted from channel key DB211 (Step S817).
[0186]The minimum thing is extracted also about a subscriber data among what has a similarly larger broadcast transmission flag than the value of member ID of the subscriber data whose member ID has processed [said] among the subscriber datas which are "1" (Step S815). Here, if there is no such subscriber data (Step S816), a subscriber data with the minimum member ID will be extracted (Step S802).
[0187]Thus, based on the channel key data and the subscriber data which were extracted, Creation/transmitting processing of the above-mentioned explanation, therefore the common control packet for channel key distribution and the individual control packet for contract information distribution is performed, and creation/transmitting processing of the common control packet of a master key creation information distribution important point is performed after that. Moving the above processing is continued without an intermission from a broadcast start.
[0188]Generation of the common control packet for channel key distribution, the individual control packet for contract information distribution, and the common control packet for master key creation information distribution can be performed in parallel. What is necessary is to perform generation/transmission control how much to create three kinds of packets every how much, respectively, and to transmit every, by the broadcast transmission control part 213, and just to generate/transmit at a fixed rate, when mounted such.
[0189]The 5th - a 7th embodiment can also be used combining an 8th embodiment so that it may understand easily.
[0190](Postscript) In broadcast with in addition few channel numbers, the limited reception according [without using channel contract information] only to a work key is also possible. Since a work key is a key set up for every channel, it can actually perform viewing-and-listening limitation only to a contractor by updating this work key during every contract term (for example, one month), and transmitting the updated work key only to the televiewer who is viewing and listening to the channel concerned during the contract term concerned as individual control information.
[0191]In such composition, when the channel key of the channel concerned has been transmitted by the common control packet, the receiving set side uses as a key the work key identifier indicated to the header part of the common control packet, and confirms whether the work key of the channel concerned exists in a work key storage. When it exists, the encryption section of the control packet concerned is decoded, and the channel key of the channel concerned is acquired. When it does not exist, the processing to the common control packet concerned is ended. Since only the viewing-and-listening contractor of the channel with the work key of the channel concerned concerned can acquire the channel key concerned from this, limited reception is realizable.
[0192]Thus, the conditional access system can only comprise updating the work key of each channel for every contract term. However, as the present CS broadcasting, when there are many channel numbers, since the update information of a work key will become large-scale if a work key is changed for every contract term, it is not so realistic. So, the method which uses together channel contract information which was explained by the above 1st - an 8th embodiment in the present CS broadcasting is desirable. However, for example, in broadcast only with one channel (or there is only one contract form), since one is enough as a work key, the conditional access

system only by the above work keys also has a merit.
[0193]The channel contract information and the work key which are memorized with a receiving set may be updated simultaneous at one individual control packet, and it may be made to update only either in a 1st embodiment and the embodiment relevant to it.
[0194]In the 1st - an 8th embodiment, when creating a digital signature, the information part which is an object of a digital signature, and the hash value as the characteristic quantity may be enciphered, and a digital signature may be created. That is, for example, as long as it is a digital signature in the contract information of drawing 5, portions and hash values other than a digital signature may be enciphered, and the digital signature of contract information may be created.
[0195]this invention is not limited to the above 1st - an 8th embodiment, and in the range which does not deviate from the gist, many things are boiled and it can be changed at an execution phase The invention of various stages is included in the above-mentioned embodiment, and various inventions may be extracted by the proper combination in two or more composition business indicated. For example, even if some constituent features are deleted from all the constituent features shown in an embodiment, The technical problem (at least one) described in the column of Object of the Invention is solvable, and when the effect (at least one) described in the column of the effect of the invention is acquired, the composition from which these constituent features were deleted may be extracted as an invention.
[0196]
[Effect of the Invention]As explained above, according to this invention, offer of the paid broadcasting service with high safety which can prevent still more unjust viewing and listening is enabled, without pressing broadcast bands by distributing a lot of individual control information, even if members increase in number.